ESX Directory Enabled Networking Guide

FORE
SYSTEMS®

MANU 0377-01

U.S. Government Restricted Rights. If you are licensing the Software on behalf of the U.S. Government (“Government”), the following provisions apply to you. If the Software is supplied to the Department of Defense (“DoD”), it is classified as “Commercial Computer Software” under paragraph 252.227-7014 of the DoD Supplement to the Federal Acquisition Regulations (“DFARS”) (or any successor regulations) and the Government is acquiring only the license rights granted herein (the license rights customarily provided to non-Government users). If the Software is supplied to any unit or agency of the Government other than DoD, it is classified as “Restricted Computer Software” and the Government’s rights in the Software are defined in paragraph 52.227-19 of the Federal Acquisition Regulations (“FAR”) (or any successor regulations) or, in the cases of NASA, in paragraph 18.52.227-86 of the NASA Supplement to the FAR (or any successor regulations).

ESX is a trademark of FORE Systems, Inc.

NT is a registered trademark of Microsoft Corporation.

FireWall-1 is a registered trademark of Check Point™ Software Technologies Inc.

In the U.S.A., you can contact FORE Systems’ Technical Support using any one of the following methods:

- You can receive online support via TACtics Online at: http://www.fore.com
- You can contact Technical Support via e-mail at: support@fore.com
- You can telephone your questions to Technical Support at: 1-800-671-FORE (3673) or +1 724-742-6999
- You can FAX your questions to Technical Support at:+1 724-742-7900

Technical support for non-U.S.A. customers should be handled through your local distributor.

No matter which method is used for support, please be prepared to provide your support contract ID number, the serial number(s) of the product(s), and as much information as possible describing your problem/question.

IMPORTANT

CAREFULLY READ THE FOLLOWING TERMS, CONDITIONS AND RESTRICTIONS BEFORE INSTALLATION AND USE OF ANY SOFTWARE PROGRAMS PROVIDED BY FORE SYSTEMS, INCORPORATED. OPENING THE SEALED SOFTWARE PACKAGE AND/OR INSTALLATION OR USE OF SUCH SOFTWARE PROGRAMS SHALL BE DEEMED ACCEPTANCE OF THESE TERMS, CONDITIONS AND RESTRICTIONS.

IF YOU DO NOT AGREE WITH AND ACCEPT THESE TERMS, CONDITIONS AND RESTRICTIONS, PROMPTLY RETURN ALL SUCH SOFTWARE AND HARDWARE PRODUCTS TO FORE SYSTEMS, INC. AND ANY FEES PAID FOR SUCH PRODUCTS WILL BE REFUNDED.

1. LICENSE

Subject to the terms and restrictions set forth in this License, FORE Systems, Inc. (“FORE”) grants a non-exclusive non-transferable (except as provided herein) license to use the software programs (“Programs”) for use with FORE and/or third party hardware products.

2. COPYRIGHT

The Programs, and all related documentation, are protected by copyright and title to all programs is retained by FORE. You may not copy or otherwise use the Programs, in whole or part, except as expressly permitted in this License. You must reproduce and maintain the copyright notice on any authorized copy you make or use of the Programs.

3. RESTRICTIONS ON USE AND TRANSFER

The Programs may be copied solely for installation and back-up purposes. You may not modify the Programs in any manner without the prior written approval of FORE. You may physically transfer the Programs and this License, along with the related FORE hardware, if applicable, to another party only if (i) the other party accepts the terms, conditions and restrictions of this License, (ii) all copies of Programs and related documentation that are not transferred to the other party are destroyed or returned to FORE, (iii) the related FORE hardware for programs designed solely to operate on FORE hardware, is also transferred to the other party, and (iv) you comply with all applicable laws including any import/export control regulations.

4. LIMITED WARRANTY

FORE warrants that the Programs will perform substantially in accordance with the accompanying documentation for a period of ninety (90) days from the date of shipment. This warranty is void if failure is the result of accident, abuse or misuse.

FORE warrants that any media on which the Programs are recorded will be free from defects in materials and workmanship under normal use for a period of ninety (90) days from the date the Programs are delivered to you. If a defect in any such media should occur during this 90-day period, the media may be returned to FORE, at 1000 FORE Drive, Warrendale, Pennsylvania 15086-7502 U.S.A., and FORE will replace the media without charge to you. FORE shall have no responsibility to replace media if the failure of media results from accident, abuse, or misuse.

The program contains third party software which is not fault-tolerant and is not designed, manufactured or intended for use or resale as on-line control equipment in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of the program could lead directly to death, personal injury, or severe physical or environmental damage (“High Risk Activities”). Accordingly, FORE and FORE's third party licensors specifically disclaim any express or implied warranty of fitness for High Risk Activities.

EXCEPT FOR THE WARRANTIES SPECIFICALLY STATED IN THIS ARTICLE, FORE HEREBY DISCLAIMS ALL EXPRESS OR IMPLIED WARRANTIES OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you. This limited warranty gives you specific legal rights, and you may also have other rights which vary from jurisdiction to jurisdiction.

5. LIMITATION OF LIABILITY

Your exclusive remedy and the entire liability of FORE related to the Programs shall be, at FORE's option: (i) refund of the price paid for the Programs, (ii) correction of the Programs so they perform as warranted, or in the case of media failure, replacement of media as provided above. In no event will FORE or anyone else who has been involved in the creation, production, or delivery of the Programs be liable for any damages, including, without limitation, direct, incidental or consequential damages, loss of anticipated profits or benefits, resulting from the use of the Programs, even if FORE has been advised of the possibility of such damages.

6. TERM

This License is effective until terminated. You may terminate this License at any time by destroying all copies of the Programs and related documentation. This License will terminate automatically if you fail to comply with any term or condition of this License, including any attempt to transfer a copy of the Programs to another party except as provided in this License. You agree that, upon such termination, you will destroy all copies of the Programs and related documentation.

7. CONFIDENTIALITY

You agree that the source code applicable to the Programs is confidential and proprietary to FORE. Accordingly, you may not decompile, reverse engineer or otherwise manipulate the Programs so as to derive such source code.

8. U.S. GOVERNMENT RESTRICTED RIGHTS LEGEND

If you are licensing the Software on behalf of the U.S. Government (“Government”), the following provisions apply. If the Software is supplied to the Department of Defense (“DoD”), it is classified as “Commercial Computer Software” under paragraph 252.227-7014 of the DoD Supplement to the Federal Acquisition Regulations (“DFARS”) (or any successor regulations) and the Government is acquiring only the license rights granted herein (the license rights customarily provided to non- Government users). If the Software is supplied to any unit or agency of the Government other than DoD, it is classified as “Restricted Computer Software” and the Government's rights in the Software are defined in paragraph 52.227-19 of the Federal Acquisition Regulations (“FAR”) (or any successor regulations) or, in the case of NASA, in paragraph 18.52.227-86 of the NASA Supplement to the FAR (or any successor regulations). Use, duplication or disclosure by the Government is subject to the restrictions set forth in such sections. The Contractor for the Programs is FORE Systems, Inc., 1000 FORE Drive, Warrendale, Pennsylvania 15086-7502.

YOUR USE OF THE PROGRAMS ACKNOWLEDGES THAT YOU HAVE READ THIS END-USER SOFTWARE LICENSE, UNDERSTAND IT AND AGREE TO BE BOUND BY ITS TERMS, CONDITIONS AND RESTRICTIONS. YOU FURTHER AGREE THAT THIS LICENSE IS THE COMPLETE AND EXCLUSIVE STATEMENT OF YOUR AGREEMENT WITH FORE AND SUPERSEDES ANY PROPOSAL OR PRIOR AGREEMENT, ORAL OR WRITTEN, AND ANY OTHER COMMUNICATIONS RELATING TO THE SUBJECT MATTER OF THIS LICENSE.

The Directory Enabled Networking(DEN) Guide provides an overview of policy administration. It covers start-up procedures, explains how to use the Policy Console, and provides detailed procedures showing how to set and administer policies. It provides troubleshooting tips to help pinpoint and resolve directory enabled network-related problems; and it describes the ESX DEN schema that is useful in understanding the lower-level characteristics of the ESX implementation of DEN.

2–Directory Enabled Networking Overview

Chapter 2, “Directory Enabled Networking Overview”, describes DEN concepts and DEN architecture. It provides information on how policies work, and it outlines the differences between global and specific policies. It also describes the basic differences in corporate organizational structures and then shows how to create a policy tree that mirrors the structure of your organization.

This chapter is organized as follows:

- Directory Enabled Networking
- Active Directory Services Agent
- Directory Enabled Networking Architecture
- Organizational Structures
- The Directory Tree
- Policies and How They Work

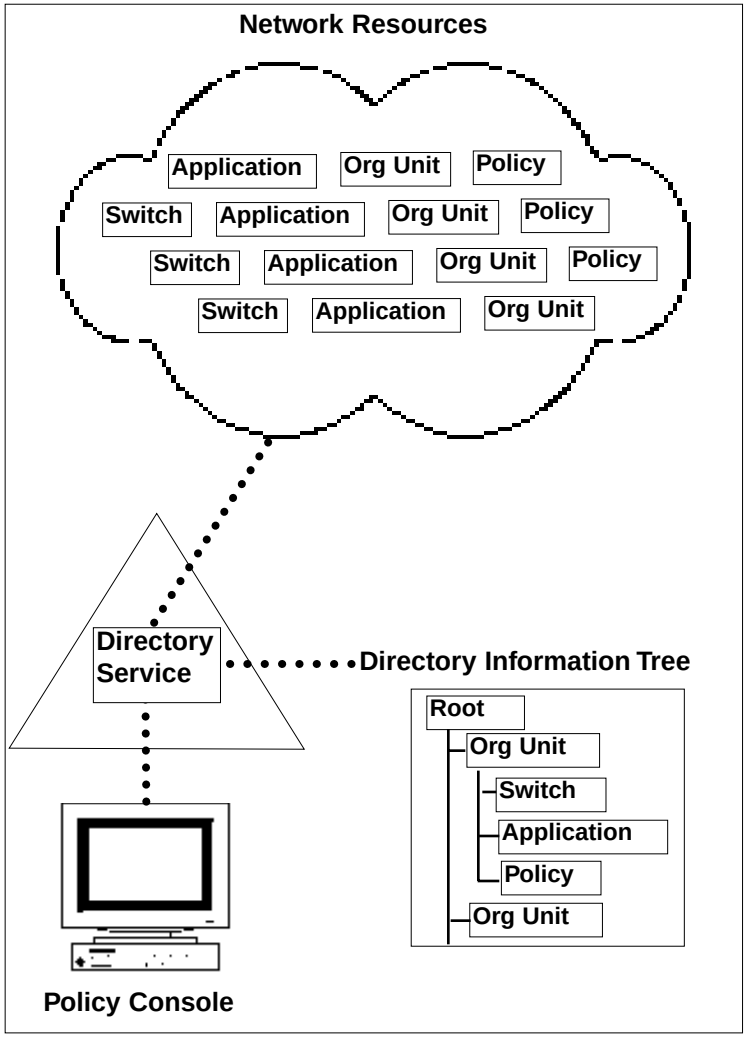
2.1 Directory Enabled Networking

Directory Enabled Networking (DEN) represents a new network model. This model allows collections of diverse network resources, which by themselves cannot interoperate, to be easily configured and managed.

How DEN Works

Key components of the DEN schema are described here and then shown in the illustration.

- *Directory Service* The directory service is a server component that manages the information describing network resources and controls access to it.
- *Network Resources* The Network resources are represented as objects in the directory information tree.
- *Directory Information Tree* The directory information tree is a hierarchical schema that models the physical data managed by the directory server.
- *Policy Console* The Policy Console allows administrators to view information and control the network by establishing policies defining how the objects in the directory behave. Administrators can control where policies are applied in the network by positioning them on the directory tree using the Policy Console.
- *Policies* A policy specifies the action that a switch will take when it detects packets of a certain type. Policies can be either specific or global:
  - *Specific policies* apply to a single network resource.
  - *Global policies* are positioned closer to the root in the directory tree and apply to the subordinate nodes.



The DEN Model

Directory Service

Under the DEN model, the directory service runs on a directory server, forming the hub of the network. It contains the meta-information, which is the common store of information describing the network, its resources, and the relationships among these resources. It provides physically-distributed, logically-centralized access to information required by the distributed systems in the network infrastructure. By providing this access to information, it allows distributed systems to work together cooperatively.

Because it maintains the persistent state of the network in a central repository that administrators can access, it provides the powerful capability of managing the network from a central location. And it provides a means for network resources to share information with each other.

Network Resources

The directory service incorporates traditional directory objects, like users and groups in its schema, along with network resources such as applications, devices, protocols, and services. Network resources use the directory service to:

- Self-identify and publish information about themselves
- Discover other resources
- Discover current information about other resources

Administrators and applications can query the directory service to make decisions about obtaining and providing services to network resources. By allowing network resources to share information and make decisions, DEN enhances the intelligence of the network.

Policies and Network Management

Network administrators control networks by defining and managing policies. In the DEN model, policies dictate and direct how network services behave. DEN provides a mechanism to create a policy once and then deploy it throughout the network. Policies reside in the directory service along with the information describing the network resources. Depending on where it is positioned on the directory tree, a policy can apply to a specific network element or to a collection of network elements.

The Directory Schema and the Directory Information Tree

The DEN Information model organizes all of the network elements–devices, applications, users, services, and policies–in a hierarchical schema within the directory service. The schema allows the network administrator to view all of the network elements and the various relationships among them.

Each directory server can support its own schema extensions or a schema based on a standard–for example, X.520, X.521, and CIM 2.0. FORE Systems has defined its own schema extensions, which can coexist with any of the standard schemas, to model and represent ESX switches. *See Appendix A–The ESX DEN Schema.*

The directory Information tree provides a mechanism that an administrator can use to control the relationship among objects by defining where policies are applied.

2.2 Advanced Directory Services Agent (ADSA)

ESX switches contain an extensible software agent, the Advanced Directory Services Agent (ADSA), that integrates the switch with the directory service and enforces policies.

ADSA Interfaces

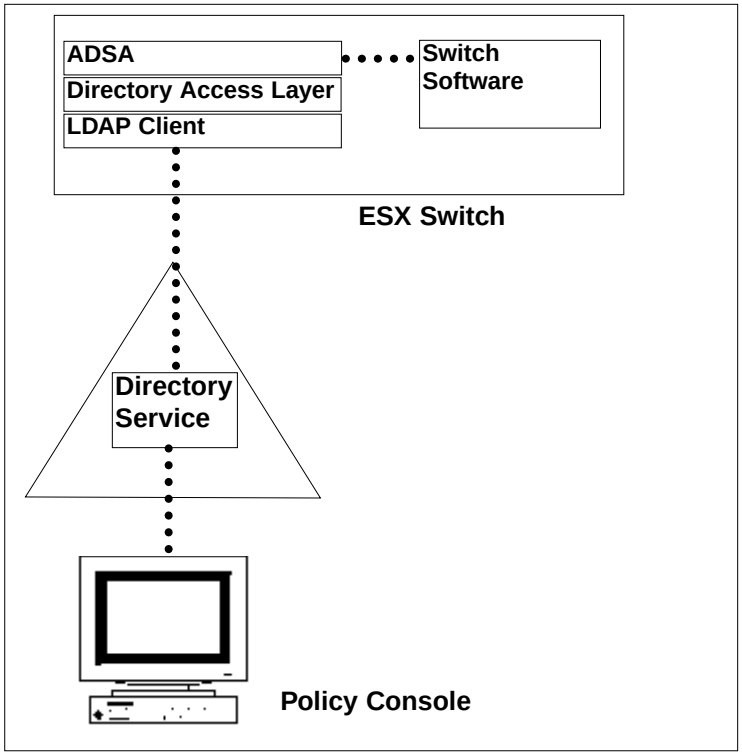
The ADSA provides the interface between the switch software and the directory access layer. The directory access layer communicates with the directory service via the Lightweight Directory Access Protocol (LDAP) client interface that, in turn, communicates with the directory service.

Note: The ADSA supports both LDAP Version 2.0 and 3.0.

ADSA Functions

ADSA provides powerful functions to integrate and synchronize the switch with the directory service. Currently, the ADSA performs the following functions:

- Maintains constant communication and stays in synchronization with the directory service
- Recognizes known LDAP directories–Netscape Directory Server and Novell NDS.
  Note: In a future release, ADSA will recognize Active Directory.
- Publishes the switch inventory, specific switch policies, and status information to the directory service
- Downloads global policies and performs switch policy conflict checking
- Enforces global policies
- Performs failure recovery



The Advanced Directory Services Agent

Note: In future releases, additional functions will be added through the extensible plug-in model.

2.3 Directory Enabled Network Architecture

A FORE Systems Directory Enabled Network is made up of these components that are also shown in the diagram and described in the following text:

- Policy Console
- LDAP Directory Server
- Directory Service
- ESX-Admin Management Station
- Directory Enabled Network Element

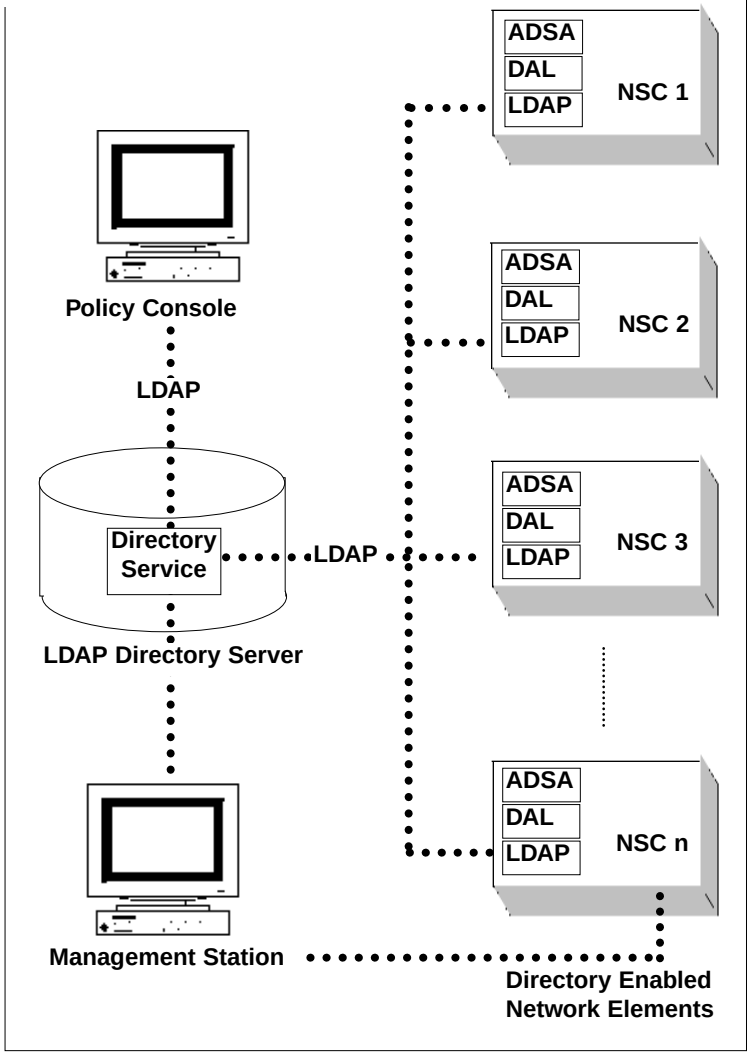
Policy Console A software application running on a workstation (NT or UNIX) that administrators use to view and configure the policies enforced within the *Directory Enabled Network*. The Policy Console communicates with the *LDAP directory server* using the LDAP protocol.

LDAP Directory Server A stand-alone server (NT or UNIX) running NDS or Netscape directory server that has network connectivity with the NSC and the *Policy Console* using the LDAP protocol. The directory server hosts the *directory service*.

Directory Service The directory service contains the meta-information, which is the common store of information describing the network, its resources, and the relationships among these resources.

Management Station A management station that connects to an NSC that can be used to create specific policies applying only to that NSC.

Directory Enabled Network Elements ESX-2400 and ESX-4800 switches with ADSA installed–that are managed by the *directory service*.



Directory Enabled Network Architecture

2.4 Organizational Types

This section describes the various ways organizations are structured and how these structures map into directories. Generally, large companies are organized in one of the following ways:

- Region or locality
- Department
- Line of business

Locality-Based Organizations

In a *locality-based* structure, organizational units report to management located in a locality or region. This structure is also known as a geographically-dispersed hierarchy.

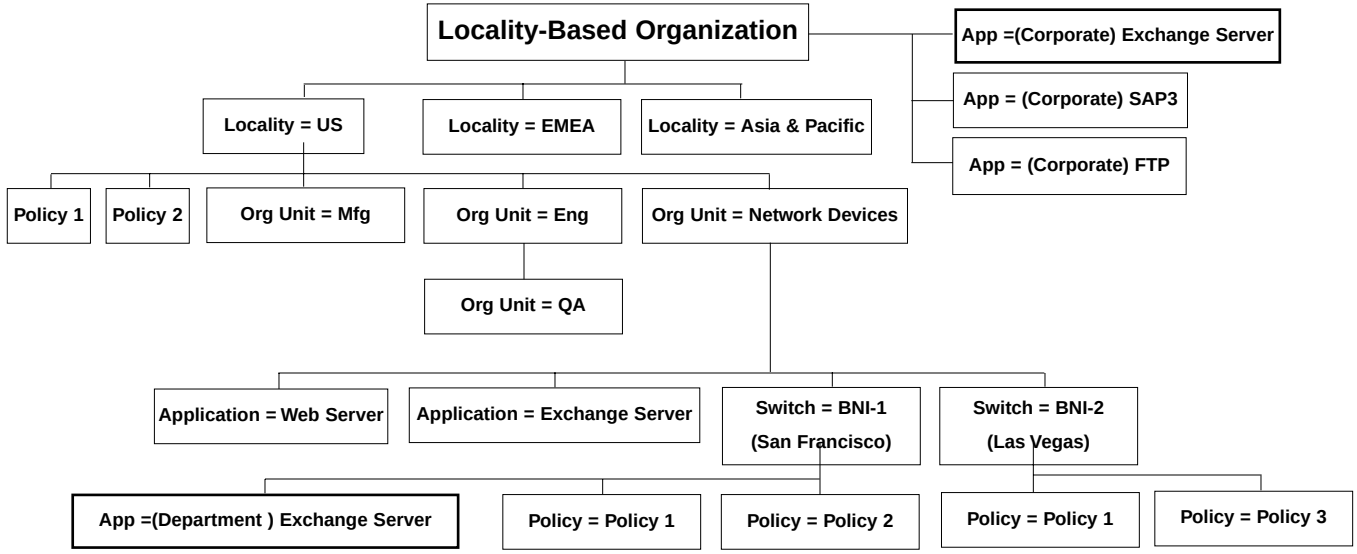
For example, a locality-based company might be organized into the following global units:

- US and Latin America
- Europe, Middle East, and Africa
- Asia and Pacific

In locality-based companies, a centralized structure coordinates the activities of the regions that operate, for the most part, as independent companies.

Departmental units would report to the regional unit. For example, the US and Latin America Region would have separate departments for Manufacturing and Engineering. These departments would operate autonomously from parallel departments that may exist in other regions.

The diagram shows network resources–switches, policies, and applications–existing at various levels in the organizational hierarchy, depending on where those resources will be applied. Note that the same application (Exchange Server) exists at both the corporate and the department level, allowing different policies to be set at different organization levels.



Department-Based Organizations

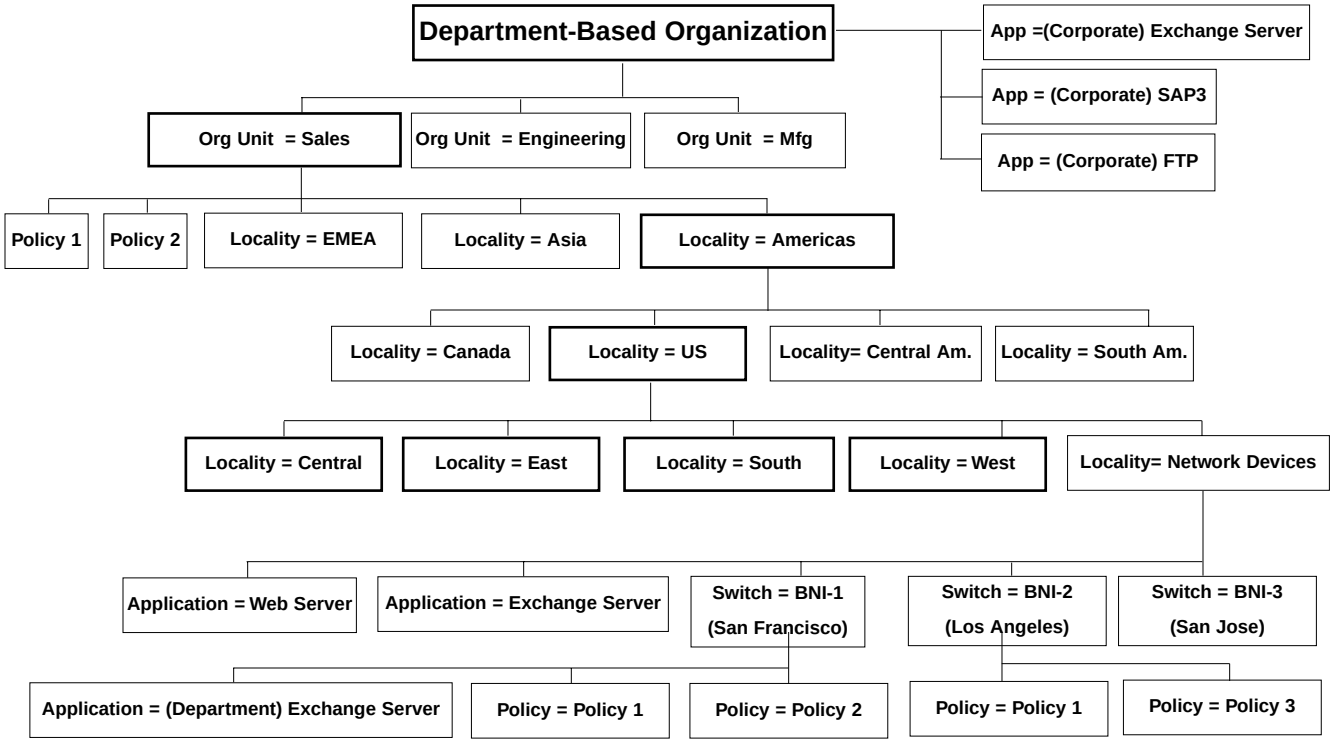
In a *department-based* structure, the organizational units, although they are located in different localities or geographic regions, report to management located in a central location.

For example,a department-based company might be organized into the following departmental units:

- Sales
- Engineering
- Manufacturing

In department-based companies, each department directs the activities that occur within the department, although the departmental personnel and offices may be globally dispersed.

For example, in a department-based organization, the sales department might be organized into global units and subdivided into regions.



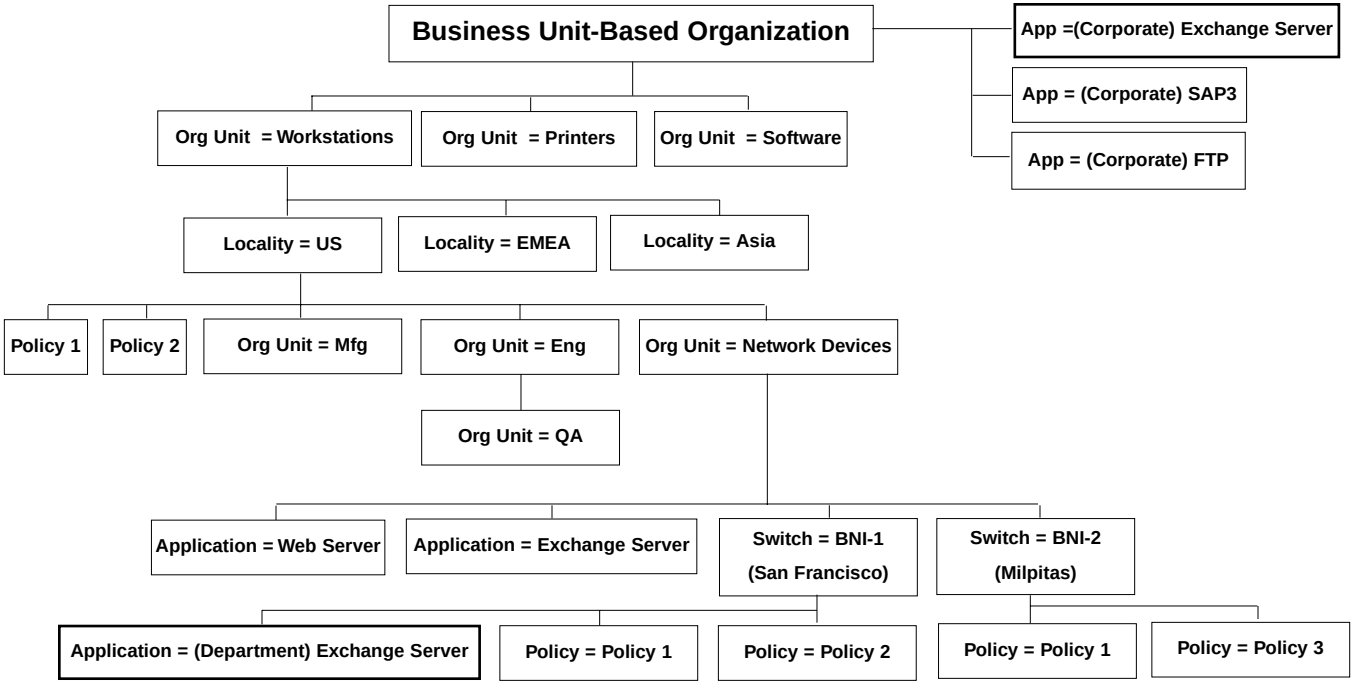
Business Unit-Based Organizations

In a *business unit-based* structure, the business is organized into a number of separate, autonomous sections that have a similar departmental structure. Generally, they report in at the corporate level.

In business unit-based companies, each business unit directs the activities that occur within the unit, although the departmental personnel and offices may be globally dispersed. *In the example, the business unit-based company is organized into Workstations, Printers, and Software, distributed globally.*

Below the organizational unit level, a business unit-based company might be subdivided by locality.–*in the example, US, EMEA, and Asia*. In addition, the localities under each organizational unit might be subdivided functionally–*in the example, Manufacturing and Engineering*.

As highlighted in the diagram, an application that exists at the corporate level–*Exchange Server*–might also exist at the local level. This allows an administrator to apply different policies for the same application at different levels in the organizational hierarchy.



2.5 The Directory Information Tree

The directory information tree is a graphical representation of network objects and their attributes that shows the relationship among those objects heirarchically. The directory information tree represents both the objects you define using the Policy Console and the objects that pre-exist in the directory server.

Before you define policies for your network, you need to define the network schema by creating network objects and organizing them in a directory tree structure subordinate to the root node. The directory tree you establish has a nodal structure similar to the structure Windows NT uses to represent the resources that are available on the network.

Network Objects

You can use the Policy Console to create objects that represent network elements. These objects are positioned below the root node in the directory, and can be nested. These network objects include:

- Geographic region (or locality)
- Organizational unit
- Switch
- Application
- Application policy

Nodes on the Tree

The directory tree has a hierarchical structure, with objects distributed as nodes. The node located at the top of the directory tree is called the *root node*, and a node which does not have any subordinates is called a *leaf node*.

Nodes can be expanded or collapsed to reveal or conceal subordinate nodes.

High-Level Directory Tree Structures

You need to take the structure of your organization into account when you create the directory tree. Directory trees for the three organizational types described previously would have the following higher-level structures:

Note: If you have an existing directory information tree structure, you may need to model your DEN tree around it.

- *Locality–Based Tree* has a node for each geographic region under the root node. For example:

Root Node

Geographic Region Nodes

- *Department–Based Tree* has a node for each organizational unit under the root node.
- *Business Unit–Based Tree* has a node for each business unit under the root node.
  Note: The tree for a business unit-based organization closely resembles a department-based organization tree.

Completing the Directory Tree

After you create icons that represent the high-level structure of your organization, you need to complete the tree by creating objects to represent:

- Organizational units and switches
- Applications and application policies

2.6 Policies and How They Work

Policies specify the actions a switch will take when it determines a certain condition exists. By creating traffic policies, you can control the flow of packets though your organization. Policies can be global or specific, depending on where you apply the policy in the network.

Layer-4 Application Class-of-Service Policies

The ADSA, running in the ESX switch, provides an application-based method of controlling the flow of packets. The ADSA recognizes application policy objects located in the directory service, and it configures the switch to enforce those policies. When the switch processes a packet, it looks for the application identifier in the packet. If a policy exists for that application, it executes the action specified by the policy on that packet.

Actions

When you create a policy, you define an action that you want the switch to take when it encounters traffic that is sent by or will be received by a specific application. The switch can take one of the following actions on traffic generated by an application; it can:

- Assign the packet a higher or lower priority
- Drop the packet
- Redirect the packet to a different destination
  Note: You can redirect a packet to a specific port on the switch–for example, to a port where a network analyzer is attached.

Policy Types

You can create specific or global policies, depending on the area of your network where you want the policy to apply:

- *Specific Policy*–a policy that you create at the switch level in the directory for a specific switch.
- *Global Policy*–a policy that you create for a node in the directory located above one or more switch objects in the directory. If you create a policy at the root level, for example, it will apply to all switches on the network.

Handling Policy Conflicts

When you establish a global policy for application, you can create either a default or an enforced global policy. If a policy conflict exists, a policy will defer to or take precedence over another policy depending on whether it is a default or an enforced global policy.

- *Default Global Policies* are overridden by specific policies.
- *Enforced Global Policies* take precedence over both specific policies and global default policies.

Policies and Application Port Numbers

A policy instructs a switch to take a certain action when it encounters a packet from a specific application. Each packet contains an application identifier or *port number*. A switch reads the port number in a packet to identify the application.

IANA maintains the list of standard application port numbers that are consistently used in all networks. For example, FTP port numbers are 20 and 21. Port numbers fall into three categories:

- Well-known
- Registered
- Private or dynamically-assigned

Note: Use IANA specified port numbers when you define port numbers for your applications. Assign a port number in the range of private or dynamically-assigned numbers to applications that are not well-known or registered.

3–Getting Started

This chapter describes how to install the Policy Console software and how to configure the directory service so that it will contain ESX specific objects. After installing the Policy Console and configuring the directory service, you will be able to use the Policy Console to create a directory tree and create policies. *See Chapters 4–6*.

This chapter assumes that you are familiar with directory server concepts like Distinguished Name (DN), Root Node, and Directory Information Tree (DIT).

Note: Although you may have already installed a directory server, this chapter provides information on installing a Novell NDS 4.11 (*see Section 3.2*) and a Netscape Directory Server 3.0 (*See Section 3.3*).

3.1 Installing the Policy Console Software

Before installing the Policy Console software, you need to verify that the PC you intend to use as a network management station meets the necessary requirements–*see Section 3.1.1*. You will install the Policy Console software using the ESX-Vision installation wizard–*see Section 3.1.2*.

3.1.1 Policy Console Software Requirements

To install Policy Console software, you must have the following hardware and software configuration on the PC you will be using as the network management station:

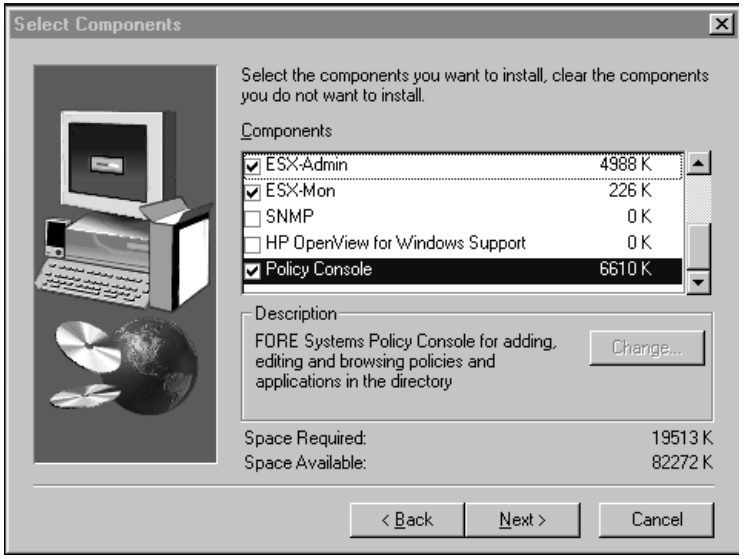
- A minimum of 64 MBytes of RAM
- A minimum of 50 MBytes of available disk space
- NT 4.0 or higher Workstation or Server
- Service Pack 3.0 or higher recommended

3.1.2 Install Directory Console Software

To install the Policy Console software:

1. Load the CD-ROM containing the ESX-Vision software into the CD-ROM drive of the PC you will be using as the network management station.
2. Open the ESX-Vision Disk 1 folder and double-click on **`setup.exe`** to launch the ESX-Vision Installation wizard.
3. During the Installation process, choose "Custom Installation":

4. After selecting Custom Installation, at a minimum, select Policy Console and then select ESX-Cli.
Note: Both Policy Console and ESX-Cli are required. If you will be communicating with an NSC directly, you may also want to install ESX-Admin and ESX-Mon.



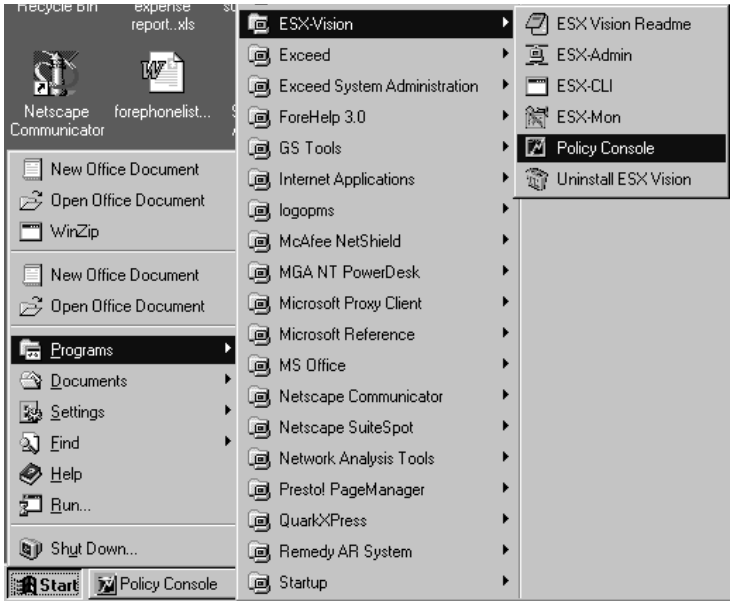
5. Follow instructions in the Installation Wizard to install Policy Console software in the Programs folder on your C drive.

Note: For detailed instruction on installing the Policy Console software on your machine, refer to *Chapter 4, "Startup"*, of the ***ESX Administrator's Guide***.

3.1.3 Launching the Policy Console Software

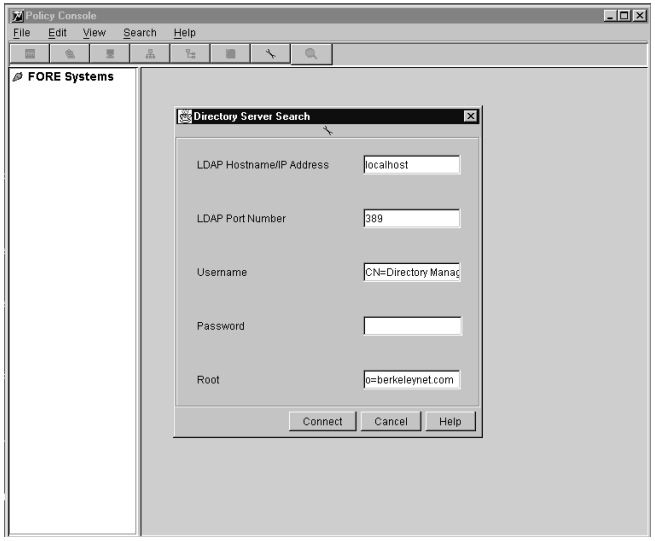
The ESX-Vision Installation wizard will install the Policy Console icon on the Start/Programs/ESX-Vision submenu. To launch the Policy Console Software and access the Policy Console, perform the following steps:

1. To launch the Policy Console software:
- Open the start menu.
- Select programs.
- Select ESX-Vision.
- Click the Policy Console icon.



After clicking the Policy Console icon, the software will display the Policy Console screen:

Next, the software will display the Directory Server Settings screen.



2. If the directory server is already installed, connect to it by filling in the information on the screen:

Parameter	Description
LDAP Hostname Address	The name of your directory server–for example: hardrock
LDAP Port Number	TCP port number on which LDAP-based directory servers listen for client connections. The default value is 389. It can be changed to a value that will be recognized by the server.
User Name	Directory Server authorized name where: cn=user name–for example: cn=directory manager.
Password	Password for user name.
Root	LDAP Path of the Root Node where o=root–for example: o=berkeleynet.com.

Note: For information on installing a directory server, refer to:

- Section 3.2 “Installing and Configuring a Novell 4.11 Directory Server (NDS)”
- Section 3.3 “Installing and Configuring a Netscape Directory Server 3.0”

After connecting to the directory server, refer to Chapters 4 – 6 for information on using the Policy Console interface, configuring a directory tree, and configuring policies.

3.2 Installing and Configuring a Novell Directory Server (NDS)

The Policy Console can communicate with both Novell NDS and Netscape Directory Servers. This section describes how to install and configure a Novell directory server.

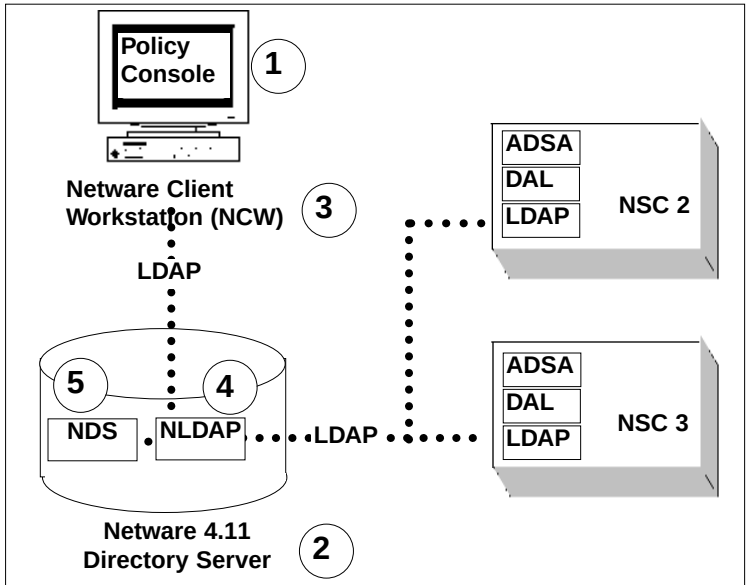
Note: If you are configuring a Netscape directory server, refer to *Section 3.3.*

The following diagram provides an overview of the Novell Directory Server Configuration. It highlights the components that need to be installed and configured.

The following sections contain step-by-step instructions that describe how to install and configure a Novell Directory Server to communicate with ESX switches and the Policy Console:

Section	Topic
3.2.1	Install Novell 4.11 Directory Server
3.2.2	Install Novell 4.11 Intranetware Client
3.2.3	Install NDS LDAP Enabler 1.0
3.2.4	Create a User in NDS–*the user you create must have supervisory access to the subtree in which you want ADSA objects to be created*
3.2.5	Add ESX Enhancements to NDS Schema
3.2.6	Add and Map Schema Attributes to LDAP
3.2.7	Add and Map Schema Class Objects to LDAP

Note: When you install the directory server, you will need to define the structure of your directory information tree. Refer to *Section 2.4* for suggestions regarding the type of tree structure that may suit your needs.



NDS Component Installation Overview

Step	Component
1	Install NDS (if you have not installed it already)
2	Install Policy Console
3	Install Intranetware Client
4	Install NDS LDAP Enabler 1.0
5	Install ESX Schema Enhancements

Novell Directory Server (NDS) Configuration

3.2.1 Install Novell 4.11 Directory Server

The first step in configuring the Novell Directory Server environment is to install a Novell 4.11 Directory Server.

Hardware and Software Requirements

Before installing and configuring an NDS Server, you must have the following hardware and software:

Hardware

- An Intel PC that will function as the Novell Intranetware Directory Server
- A Windows NT PC that will function as the Netware Client Workstation

Software

- Internetware 4.11 NDS Directory Server software from Novell
- Novell 4.11 Internetware Client software
- Novell NDS LDAP Enabler 1.0 software
- ESX-Vision Policy Console and ESX-Cli software

Installing the Directory Server

Refer to the Novell 4.11 NDS manual for instructions on installing the Novell 4.11 NDS Directory Server software on a Windows NT PC.

Collecting Server information

After installing the server, collect the following information about the server. This information will be required when you configure switches to recognize the directory server. *See Section 3.5.*

- Server Name _____
- Port No. _____
- LDAP Distinguished Name User _____
  Note: This user must have administrative access.
- Password _____
- Root Server of the DIT _____

3.2.2 Install Novell 4.11 Internetware Client

To communicate with and configure NDS, you need to install a Novell Internetware Client on a Windows NT PC.
Refer to the NovelL 4.11 Internetware Client manual for installation instructions.

You can install the client on the same PC where you installed the Policy Console and ESX-Cli software, although this is not required. If you install the Policy Console and ESX-Cli software on a separate network management station, it must have network connectivity to the Novell server.

3.3 Install NDS LDAP Enabler 1.0

FORE Systems ESX switches communicate with the directory server using the LDAP protocol. To allow the NDS to communicate with ESX switches, you must install the NDS LDAP Enabler 1.0 on the NDS.

You can install the NDS LDAP Enabler 1.0 software from a Windows NT machine, or you can download NDS LDAP Enabler 1.0 software from the Novell website.

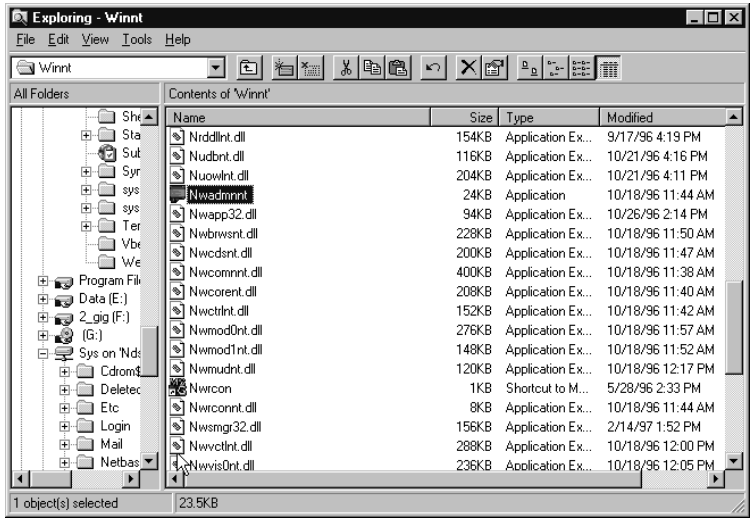
Note: The installation instructions are included with the installation file.

3.2.4 Create an LDAP User Distinguished Name

After you install the NDS LDAP Enabler 1.0, perform these steps on the Novell Client Workstation (NCW) to create an LDAP user Distinguished Name (DN):

1. Open NWADMIN and create an LDAP user DN who will have administrative access to the NDS tree. Refer to the Novell NDS documentation for instructions.

Note: It is important to record the LDAP User DN because ADSA logs into NDS directory as this proxy user. Record the name under the Collecting Server Name Information heading *See Section 3.2.1.*



2. Add the LDAP user DN as the trustee of the two new objects in the NDS tree: **`LDAP Server`** and **`LDAP Group`**.
   Note: Now that the **`LDAP Server`** and **`LDAP Group`** objects exist, LDAP–based applications, like ADSA will be able to add objects, modify objects and delete objects from NDS.

3.2.5 Add ESX Enhancements to NDS Schema

After you create an LDAP User, perform the following steps to add ESX enhancements to the NDS Schema:

1. Locate all of the schema enhancement files.
   Note: When you installed the Policy Console, these files were copied to the policyconsole\schema\NDS subdirectory of the ESX-Vision installation directory:

File	***Contains***
bniatt.sch	All ADSA specific attributes
bniapp.sch	The object class definition of ADSA BNIApplicationProcess
objectbnisw.sch	The object class definition of ADSA BNISwitch
objectbniacos.sch	The object class definition of BNISwitch–a CoS policy object

2. Copy these files to the NCW.
   Note: If you installed the Policy Console onto a workstation that had Novell 4.11 Intranetware installed, you do not need to copy the files. They can remain in their original directory.

3. On the NCW, Locate the following Novell utility:
   `nsdsch.exe`
   Note: `nsdsch.exe` is normally located in the directory: <Server>:/SYS/Public.

4. Open a DOS window and run the following commands from a DOS prompt, where:
   - **`M:`**: is your Novell server drive mounted at SYS.
   - **`<CR>`** at the end of each command line indicates you should press the carriage return key.

```
M:\Public>ndssch C:\Programfiles\Fore\ESX-Vision\DirConsole\Schema\NDS\bniatt.sch<CR>

M:\Public>ndssch C:\Programfiles\Fore\ESX-Vision\DirConsole\Schema\NDS\bniapp.sch<CR>

M:\Public>ndssch C:\Programfiles\Fore\ESX-Vision\DirConsole\Schema\NDS\bnisw.sch<CR>

M:\Public>ndssch C:\Programfiles\Fore\ESX-Vision\DirConsole\Schema\NDS\bniacos.sch<CR>
```

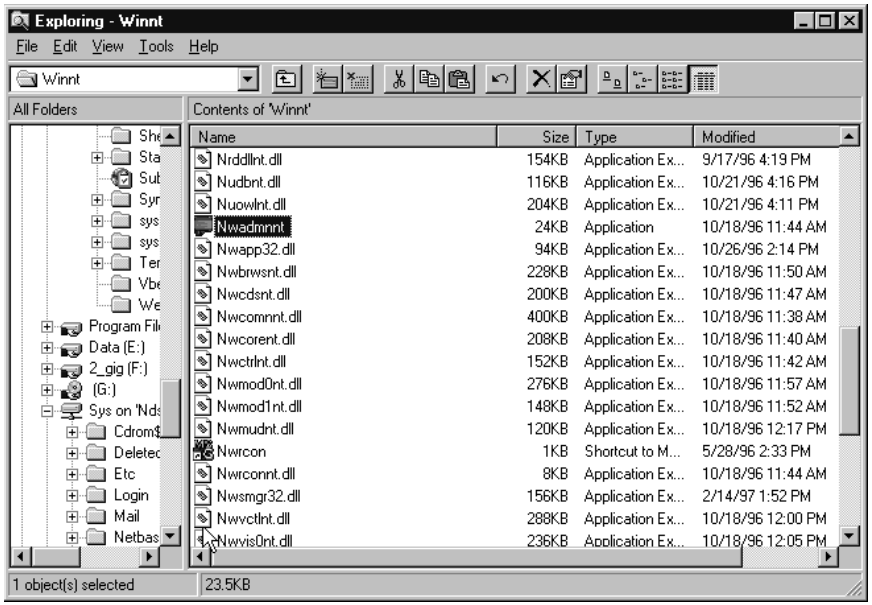
   Note: Now all the schema enhancements are known to NDS.

3.2.6 Map Schema Enhancements to the Attributes in the LDAP Enabler

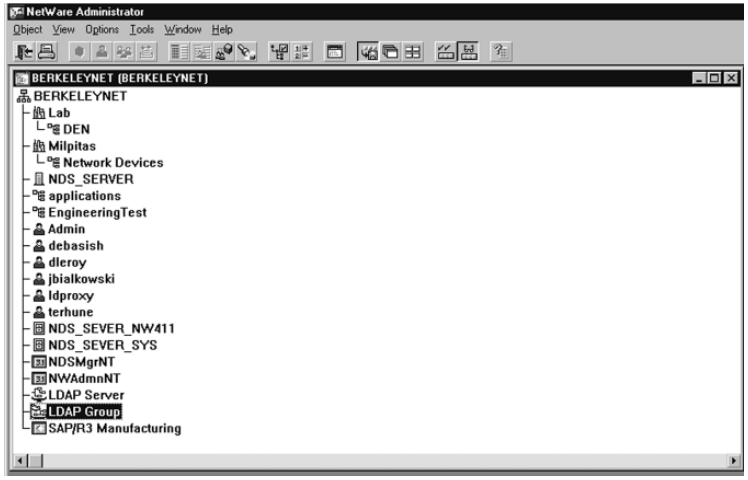
After the schema enhancements are known to NDS, the next step is to map the schema enhancements to the attributes and object classes in the Netware LDAP Enabler 1.0.

Note: This step must be performed manually. At this time, Novell does not support dynamic schema enhancements using LDAP V3 API. To map the schema enhancements to the attributes and object classes, perform the following steps:

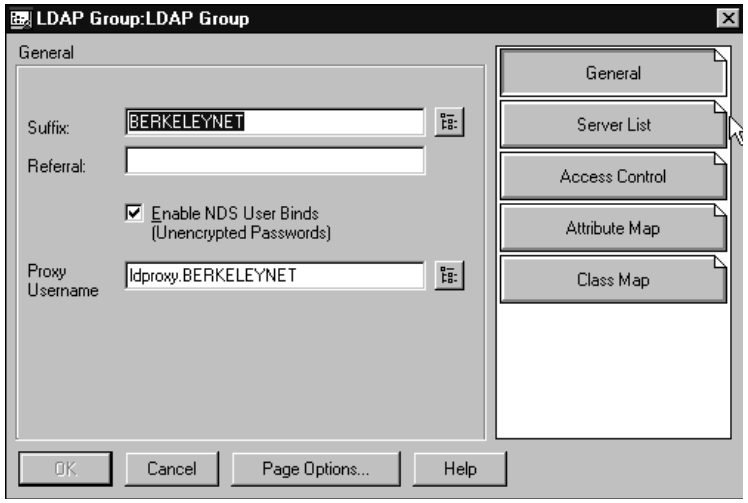
1. Double-click the **`Nwadmnt.exe`** icon on the NCW PC.



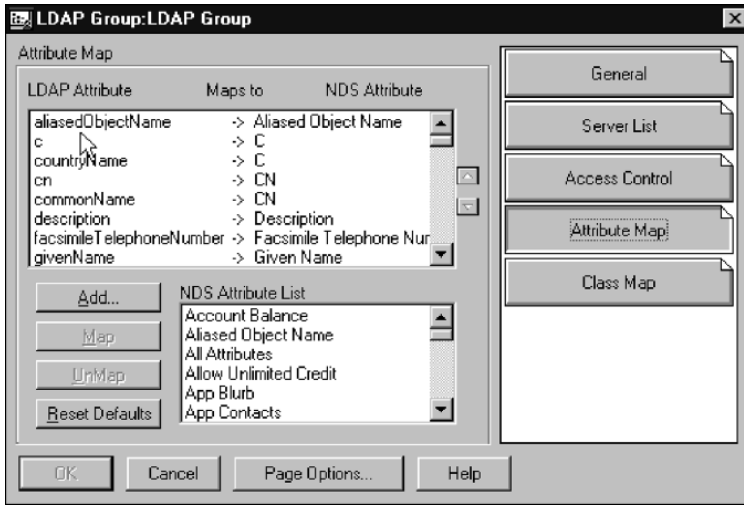
2. Double-click on the LDAP Group icon to display the LDAP Group:LDAP Group General tab page.



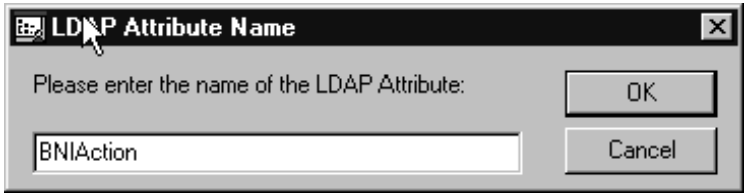
3. On the General tab page, click on the Attribute Map button to display the Attribute Map tab page.



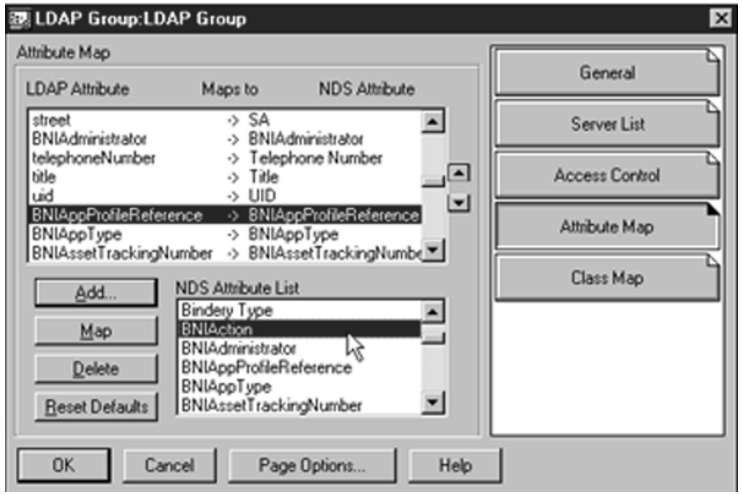
4. On the Attribute Map tab page, click the Add button to display the LDAP Attribute Name dialog box.



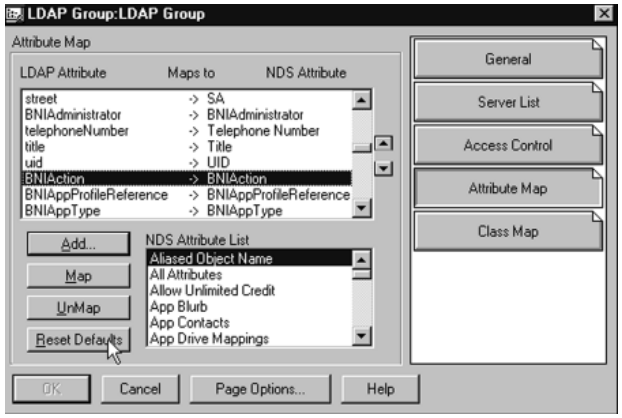
5. On the LDAP Attribute Name dialog box, type the name of a BNI attribute–*BNIAction in the example*. Then click OK to redisplay the Attribute Map page with the new attribute displayed in the NDS Attribute List–*BNIAction in the example*.



6. Scroll down the NDS Attribute List and highlight the new attribute (BNIAction), activating the Map button.

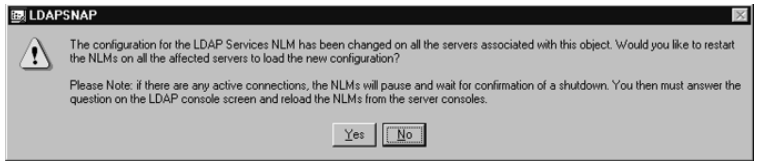


7. Press the Map button to map the new attribute.
   Note: Notice that BNIAction now appears highlighted in the Attribute map window and is mapped–*the LDAP Attribute maps to NDS Attribute.*



   Note: Do not try to map multiple attributes in one shot because the LDAP snap-in has a bug and incorrectly maps the attributes. Until a patch is available from Novell, map the attributes one at a time.

8. On the Attribute map window, click OK to display a popup window.



9. Click the Yes button on the popup window to save the mapped attribute and restart the NLDAP module.
   Note: If a prompt is not displayed, issue the following commands from the NCW workstation to restart the NLDAP module:
   1. **`unload`** NLDAP
   2. **`load`** NLDAP

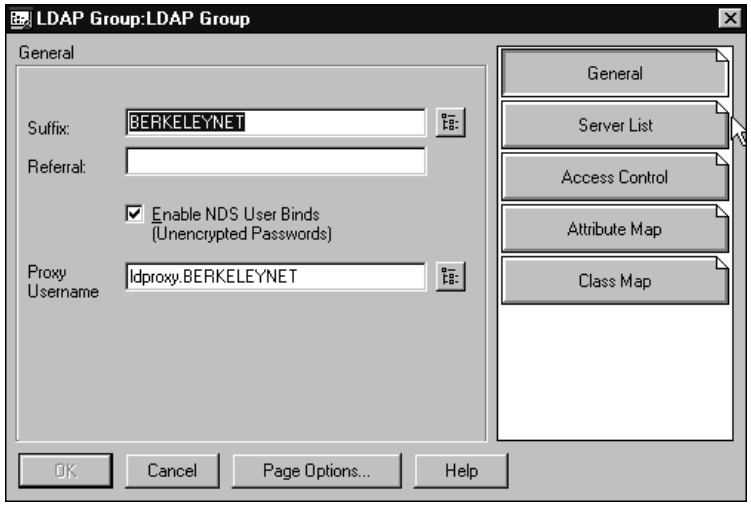
10. Repeat steps 2–9 to map each of the following ESX attributes:

LDAP Attribute	***NDS Attribute***
BNIAction	BNIAction
BNIAppProfileReference	BNIAppProfileReference
BNIAppType	BNIAppType
BNIAssetTrackingNumber	BNIAssetTrackingNumber
BNIAssetType	BNIAssetType
BNICaption	BNICaption
BNIClientPorts	BNIClientPorts
BNICopyRedirSize	BNICopyRedirSize
BNIOwner	BNIOwner

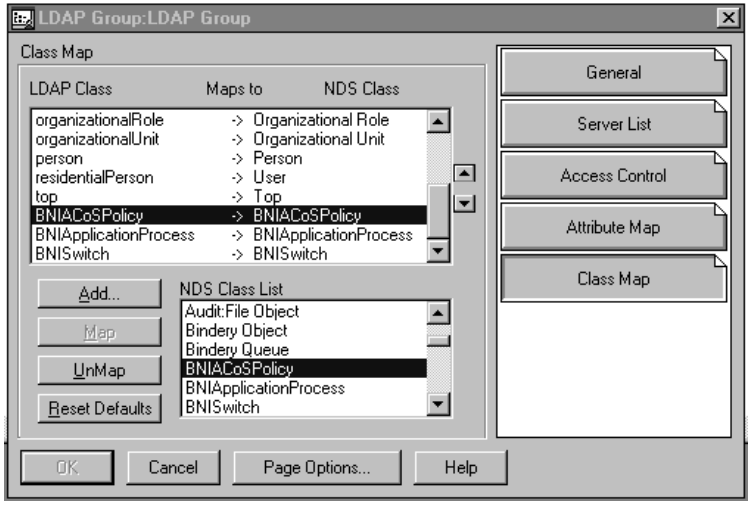
3.2.7 Map Schema Enhancements to the Class Objects in the LDAP Enabler

After you add and map all the ESX attributes–*LDAP Attributes map to NDS Attributes*–follow this procedure to add and map the ADSA specific class objects from LDAP to NDS, one at a time:

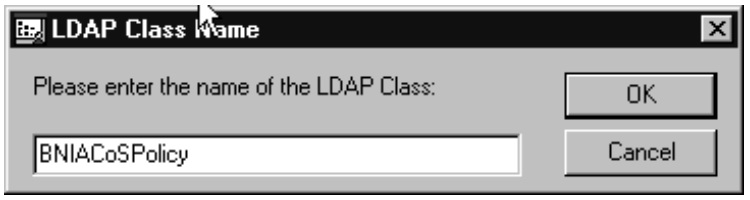
1. Starting from the LDAP Group:LDAP Group General tab page, click the Class Map button to display the Class Map tab page.

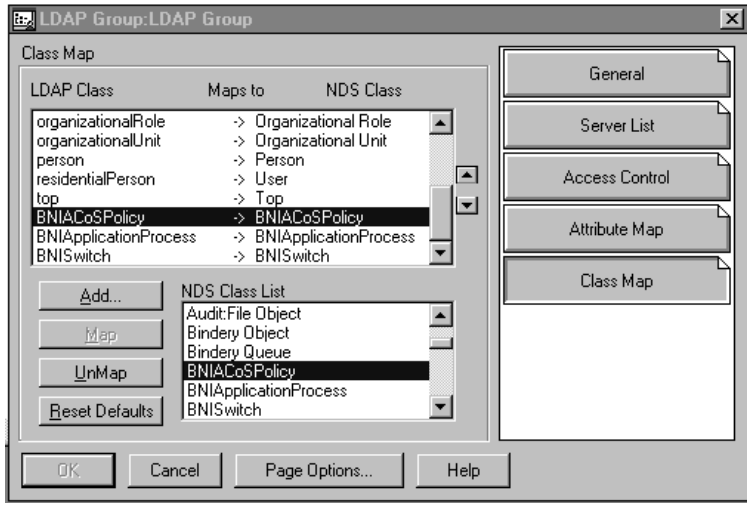


2. On the Class Map tab page, click the Add button to display the LDAP Class Name dialog box.



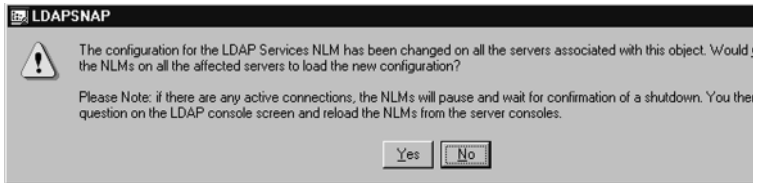
3. On the LDAP Class Name dialog box, type the name of a BNI attribute–*in the example, BNIACosPolicy*. Then click OK to redisplay the Class Map page with the new attribute displayed in the NDS Class List–*in the example, BNIACosPolicy.*





4. Scroll down the NDS Class List and select BNICoSPolicy to activate the MAP button.
5. Click the Map button to map the BNICoSPolicy object.

   Note: Do not try to map multiple objects in one shot because the LDAP Snap-in has a bug and incorrectly maps the objects. Until a patch is available from Novell, map the objects one at a time.
6. On the Class map window, click OK to display a popup window.



7. Click the Yes button on the popup window to save the mapped object and restart the NLDAP module.
   Note: If a prompt is not displayed, issue the following commands from the NCW workstation to restart the NLDAP module:
   1. **`unload`** NLDAP
   2. **`load`** NLDAP
8. Repeat Steps 1–7 for each of the following object classes:

LDAP Object Class	***NDS Object Class***
BNIACoSPolicy	BNIACoSPolicy
BNISwitch	BNISwitch
BNIApplicationProcess	BNIApplicationProcess

Verify that the NDS Enhancement Was Successful

After adding ESX enhancements to the NDS schema and mapping the attribute and objects, you can verify that the NDS enhancement was successful by performing the following test:

1. Start the Policy Console.
2. Connect to the NDS LDAP Enabler.
3. Create a switch object under any pre-existing folder or create a new folder–for example, Network Devices.
   Note: If you were able to create a switch object successfully, the NDS schema enhancement was successful.

3.3 Configuring a Netscape Directory Server

The Policy Console can communicate with both Novell NDS and Netscape Directory Servers. This section describes how to install and configure a Netscape directory server.

Note: If you are configuring a Novell directory server, refer to *Section 3.2.*

The following diagram provides an overview of the Netscape Directory Server Configuration. It highlights the components that need to be installed and configured.

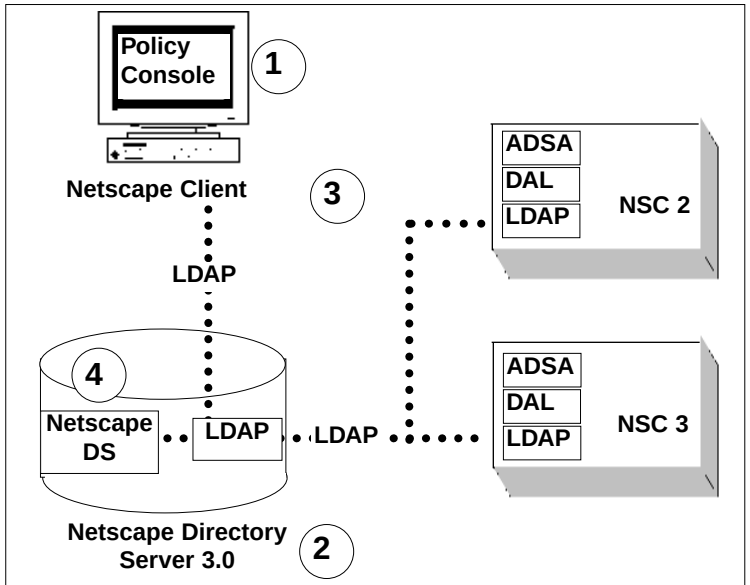
The following sections contain step-by-step instructions that describe how to install and configure a Netscape Directory Server to communicate with ESX switches and the Policy Console:

Section	Topic
3.3.1	Install the Netscape Directory Server
3.3.2	Add ESX Enhancements to the Netscape Schema

Note: When you install the directory server, you will need to define the structure of your directory information tree. Refer to *Section 2.4* for suggestions regarding the type of tree structure that may suit your needs.

3.3.1 Install the Netscape Directory Server

To install the Netscape Directory Server 3.0, refer to the Netscape Directory Server 3.0 manual.



NDS Component Installation Overview

Step	Component
1	Install Netscape Directory Server
2	Install Policy Console
3	Install Schema Enhancements

Netscape Directory Server Configuration

Hardware and Software Requirements
Before installing and configuring a Netscape directory server, you must have the following hardware and software:

Hardware

- A Windows NT PC that will function as the Netscape Directory Server
- A Windows NT PC that will function as the Netscape Client Workstation

Software

- Netscape Directory Server 3.0 software
- Netscape Client software
- ESX-Vision Policy Console and ESX-Cli software

Note: The Netscape directory server can communicate with ADSA using the LDAP protocol. No special configuration is required.

Collecting Server information
After installing the server, collect the following information about the server. This information will be required when you configure switches to recognize the directory server. *See Section 3.5.*

- Server Name _____
- Port No. _____
- LDAP Distinguished Name User _____
  Note: This user must have administrative access.
- Password _____
- Root Server of the DIT _____

3.3.2 Add Schema Enhancements

Follow instructions in this section to add schema enhancements to the Netscape directory server. To perform this step, you will locate the files that were copied during the Policy Console installation and then copy these files to the Netscape directory server.

1. On your Policy Console, locate the following files in the Schema/ Netscape subdirectory of the ESX-Vision installation directory that were created when you installed the Policy Console:
   slapd.user_at.conf: ESX ADSA attributes
   slapd.user_oc.conf: ESX ADSA object classes
2. Copy these files to the following location on the Netscape directory server: /slapd-<machine name>/config directory.
   Note: If you have modified the slapd.user_at.conf and slapd.user_oc.conf files, you must:
   1. Make a temporary copy of the modified slapd.user_at.conf file in C:\TEMP
      and
   2. Copy the temp file to the end of the pre-existing slapd.user_at.conf file located in the config directory.
   3. Repeat Steps 1 and 2 for slapd.user_oc.conf file.
3. After copying the files, restart the Netscape Directory Server.

After the restart, the directory server will recognize the new attributes and object classes. Now your Netscape Directory Server is ready for ESX ADSA.

3.4 Creating Switch Objects Representing Physical Switches (optional)

This section describes a recommended, but optional, procedure for creating switch objects using the Policy Console. Using the Policy Console, you can create all the switch objects at once, and you can position them in the desired location on the directory information tree.

Note: If you don't create switch objects using the Policy Console, the ADSA component on the NSC will do it automatically.

Before creating switch objects, you need to follow the DIT structure that your organization is using or wants to adopt. After you create the switch objects, you can start ADSA on all the switches.

To create switch objects:

1. On the Policy Console, connect to the directory server.
2. Select the node (locality or organizational unit) in the directory tree where you want to position the switch object that you will create
   Note: If the right node does not exist, you may have to create it. Refer to Section 3.5 for information on creating a folder for a switch object using ESX-Cli.
3. Click the Create Switch icon located on the icon bar at the top of the screen to display the Switch configuration page.
4. On the Switch configuration page, enter the name of the switch.
   Note: When you name the switch, you may want to follow a corporate device naming scheme–either location-based or department-based.

3.5 Configuring Switches to Recognize the Directory Server

During the final stage in Getting Started, you will configure the switches to recognize the directory server. When this step is complete, the ADSA on the NSC will be able to communicate across an LDAP interface with the directory server.

Before you perform this procedure, you may need to refer to the information you gathered in *Section 3.2* or *Section 3.3* that defines key directory server information:

- Server Name _____
- Port No. _____
- LDAP Distinguished Name User _____
  Note: This user must have administrative access.
- Password _____
- Root Server of the DIT _____

Enable ADSA on the NSC

You will use ESX-Cli to enable ADSA on the NSC.
ESX-Cli was installed earlier when you installed ESX-Vision and Policy Console on your network management station.

Repeat these steps for each switch that you are configuring:

1. On the network management station's Start menu, select Programs/ESX-Vision/ESX-Cli to display an ESX-Cli screen with an ESX-Cli command prompt: **`CLI>`**

2. Issue the following ESX-Cli configuration command string to enable ADSA on the NSC:

   CLI> cfg adsa directory-server <server name> user-dn <user dn> password <password> switch-dn <switch dn>

   The **<switch dn>** parameter must be defined to locate the switch at the correct location in the DIT. For example,a switch DN (distinguished name) could have the following configuration:

   `<OU=Network Devices, OU=Manufacturing, L=West Coast, O=Acme.com>`

   where:

OU= Organizational unit
L= Locality
O= Organization

Note: The folder in which the switch object will be placed must exist or be created before you issue the **start adsa** command. For **<switch dn>** in the previous example, the following folder must exist:

`OU=Network Devices, OU=Manufacturing, L=West Coast, O=Acme.com`

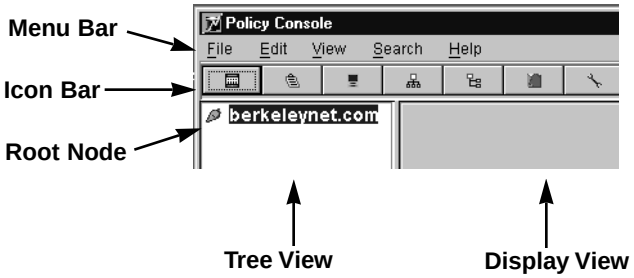
If you created a switch object for **<switch dn>** in Section 3.4, the folder was already created.

3. Issue the following ESX-Cli command to bring up ADSA on the NSC:

   CLI> start adsa

Chapter 4–Using the Policy Console Interface

When you launch the Policy Console, you will see the following display:



Menu Bar and Icon Bar
The Policy Console interface provides a *menu bar* and an *icon bar*. They allow you to create, name, and delete objects, configure policies, and position objects along the tree.

Root Node
When you start the Policy Console, the root node of your Directory Information Tree will appear at the top of the tree view, as shown in the previous diagram.

Note: You can rename the root node during installation.

Tree View
The tree view displays the root node and all the objects that have been created underneath it. When you create an object, the object appears underneath the object that is highlighted in the tree view.

Display View
The display view displays configuration pages that you will use to create new objects and their attributes. When you select an existing object on the tree, the Policy Console displays the configuration page showing the current attributes for that object.

Creating an Object
To create an object:

1. Select an item on the tree, highlighting it.
2. Click an icon on the icon bar.
   or
   Pull down the file menu on the menu bar. Then select the new object and the name of the object you want to create. *The object's attribute configuration page will appear in the display view.*
3. Supply the required attribute information on the configuration page to create the object.
   An icon representing the object will appear in the tree view underneath the object that was selected when you created it.

Deleting an Object
To delete an object:

1. Select an object on the tree, highlighting it.
2. Pull down the Edit Menu and select Delete.

Note: You can't delete an object that has other objects underneath it. You must delete all the subordinate objects first.

Chapter 5–Creating a Directory Tree

After installing a directory server and adding and mapping ESX schema extensions, as described in Chapter 3, you are ready to create a directory tree that describes the structure of your organization.

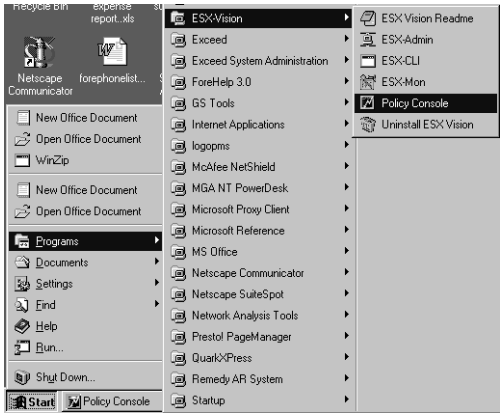
This chapter shows how to use the Policy Console to create, name, and position the objects that represent the components of the locality-based organization described in Section 2.4. In the process, the chapter shows how to build the directory tree that represents the example organization.

The following sections describe how to create the objects that make up a directory tree.

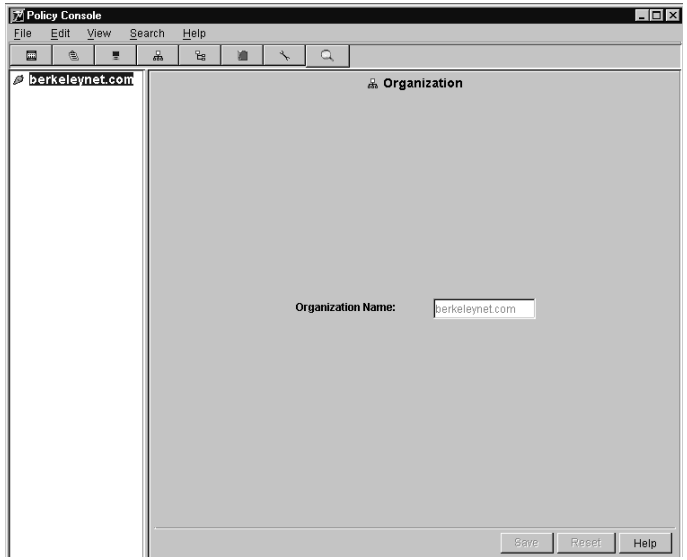
Section	***Contents***
5.1	Creating Locality Objects
5.2	Creating Organizational Unit Objects
5.3	Creating Switch Objects
5.4	Creating Application Objects
5.5	Creating Policy Objects

Launching the Policy Console

After you install the Policy Console, described in Section 3.1, you can launch it from the Start menu, as shown in the following illustration.



When the Policy Console launches for the first time, it displays a splash screen momentarily. Then it displays a tree view with the root node that you defined during installation. *See the following illustration.*



5.1 Creating Locality Objects

When you create a directory tree for a locality-based organization, the first task is to create localities under the root.

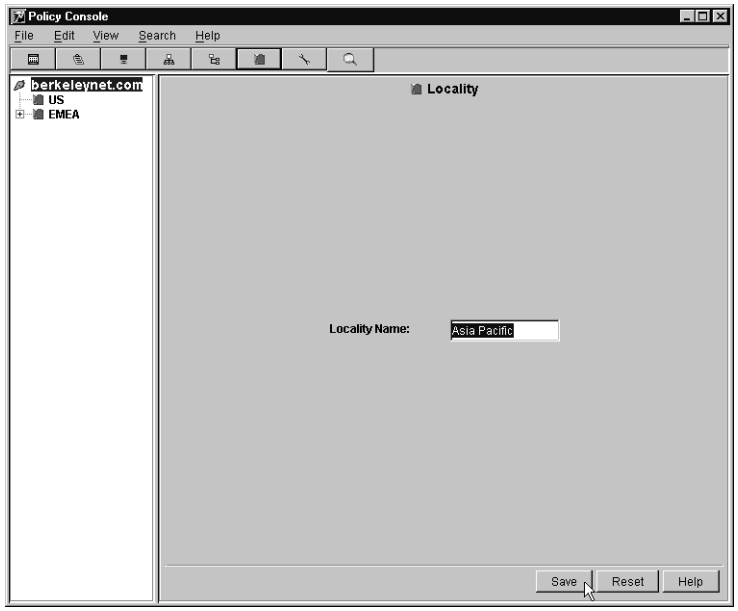
In the locality-based organization example, described in Section 2.4 and created in in Section 5, there are three global localities: US, EMEA, and Asia & Pacific.

To create a locality:

1. Select a node–*in the example, the first locality (US) is below the root node.*
2. Click the Locality icon on the Icon bar to display the locality page.
3. Enter the locality name in the Locality Name field–*in the example, the first locality is US.*
4. Click Save to create the locality object.

Note: Repeat Steps 1–4 to create the other localities: EMEA and Asia & Pacific.

Note: As you move the mouse along the Icon bar, the popup windows that appear identify the function of the icons.



Note: In the example, three global localities were created.

5.2 Creating Organizational Unit Objects

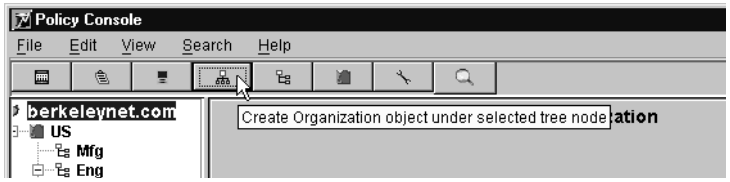
After you finish creating policies at the regional level, create the organizational units underneath them.

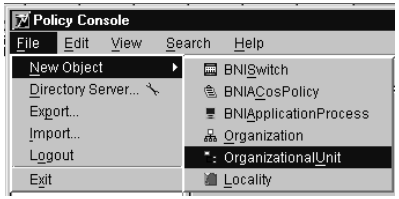
Note: You can create an organizational unit container for shared devices to simplify the management of switches that are available to all of the organizational units in the region, as shown in the example.

To create an *organizational unit* object:

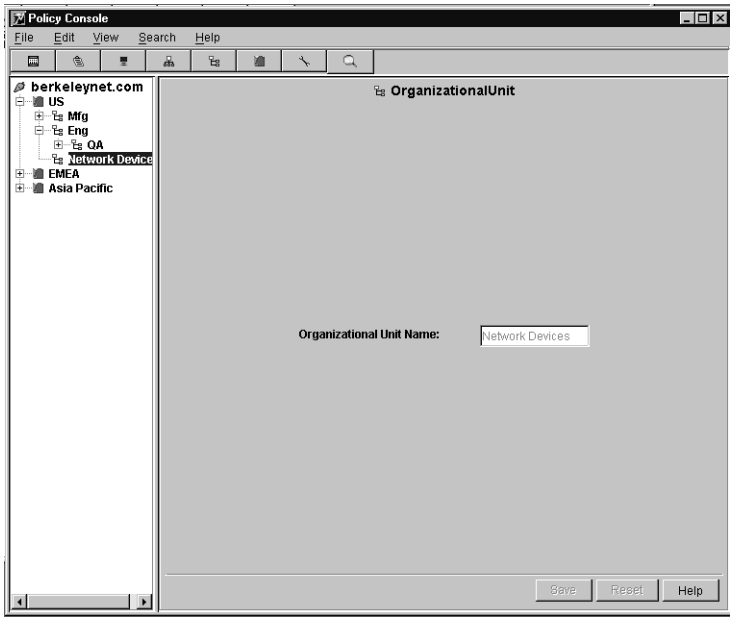
1. Select a locality node (US in the example).
2. Click the organizational unit icon on the icon bar to display the organizational unit page.
3. Enter the organizational unit name in the Organizational Unit Name field–in the example, Mfg is the first organizational unit.
4. Click Save to create the organizational unit object.
5. Repeat Steps 1–4 to create the Eng and Network Resources organizational unit objects.
6. Select the Eng organizational unit node and repeat steps 2–4 to create the QA organizational unit object below it.

Note: If your root node is a country object, you may need to create an organization object underneath it to model a locality based organization *See Section 2.4.* Select the root node, then access the Organization object icon from the menu pull-down or menu bar.





Note: You can also create an object, by selecting New Object and the object type from the menu (Organizational Unit in the example



Note: In the example, three organizational unit objects were created under the US locality object: Mfg, Eng, and Network Devices. One organizational unit object (QA) was created under the Eng organizational unit object.

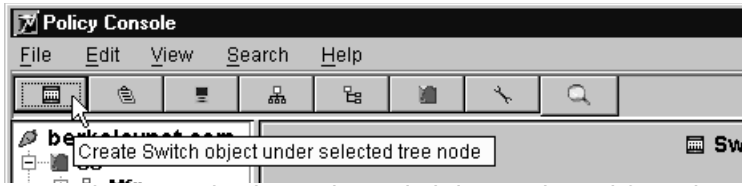
5.3 Creating Switch Objects

After you finish creating the organizational structure of the locality, you can create the switches, applications, and policies below the locality and organizational unit nodes.

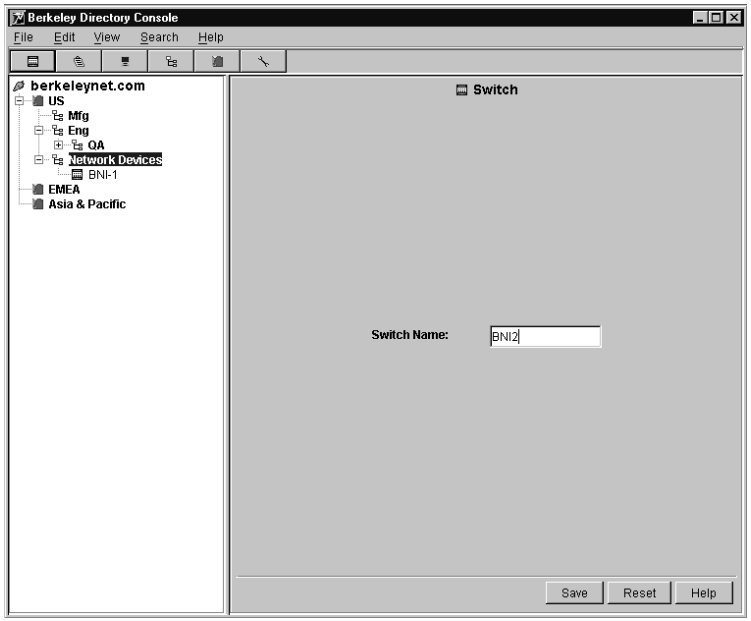
In the example, we will create the switch objects first, placing them under the US/Network Devices organizational unit.

To create a switch object:

1. Select a locality or organizational unit node–*in the example, the Network Devices organizational unit node.*
2. Click the switch icon on the menu bar to display the Switch page.
2. Enter the switch name in the Switch Name field–*in the example, BNI1 is the first switch.*
   Note: The switch name must correspond to the name you give to the switch when you configure it during the Getting Started sequence–*see Section 3.4, "Creating Switch Objects Representing Physical Switches"*.This can be done either before or after you create the directory tree.
4. Click Save to create the switch object.
5. Repeat Steps 1–4 to create the BNI2 Switch object and place it under the Network Devices organizational unit on the directory tree.



Note: The example shows the Switch icon selected from the Icon bar



Note: After you configure a switch or select a switch icon, the Policy Console displays the persistent state of the switch object in the Display View.

5.4 Creating Application Objects

An application object represents an application and its attributes. Application objects have three attributes:

- Application name
- Application protocol
- Application port number

When you create an application object, you can allow or restrict access to an application. This restriction depends on where you position the object on the directory tree.

- When you place an application object at the root level in the directory tree, you make the application accessible to all network nodes.
- When you place an application object under a locality, organizational unit, or switch object, you restrict the application to a locality, organizational unit, or switch.

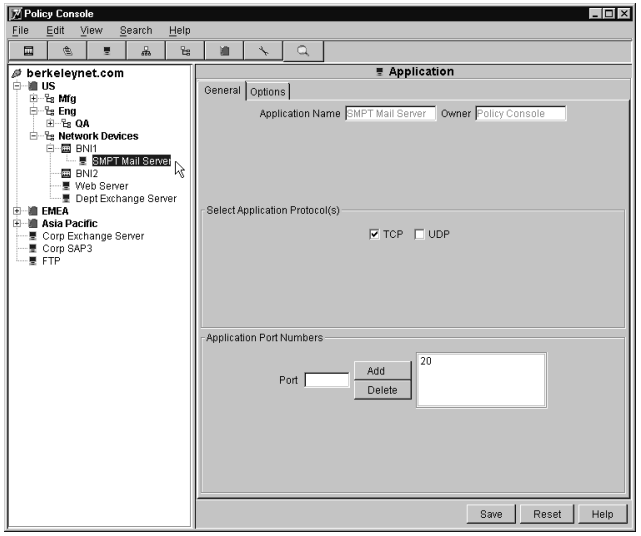
Note: The ESX DEN schema tracks application objects by name. This allows you to create multiple application objects, assign them different port numbers, position them at different levels on the directory tree, and set a policy for that application by creating a single policy object. *See Section 5.5, “Creating Policy Objects”, for details*.

5.4 Creating Application Objects-(continued)

To create an application object:

1. Select a node–*in the example, the root node is the first node with an application below it.*
2. Click the application icon on the icon bar to display the Application page.
3. Enter the application name in the Application Name field–*in the example, Corp Exchange Server is the first application under the root node.*
4. Enter the required parameters on the Application page:
   - Select Enabled (the default setting).
   - Select the Application Protocol (TCP).
   - Enter the application port number and click Add.
5. Click Save to create the application object.
6. Repeat steps 1–5 for the Corp SAP3 and FTP applications.
7. Select the Network Devices organizational unit node and then repeat steps 2–5 for the Web Server and Department Exchange Server applications.
8. Select the BNI1 switch node and then repeat Steps 2–5 for the SMTP Mail Server application.

Note: Port numbers are defined by IANA. Refer to the IANA standard when defining port numbers for your applications. Well-known and registered applications use standard *port numbers* that are consistently used in all networks. For example, FTP is a well-known application. Its port numbers are 20 and 21. Use private or dynamic port numbers for applications that are not well-known or registered.



Parameter:	Description
Application Name	Name of the application–for example, HTTP
Protocol	Protocol the application will run under
Port numbers	Enter the port number of the application There are three application port number categories: • Well-known: 1- 1023 • Registered: 1024– 49152 • Private or dynamic: 49152– 65535

5.5 Creating Policy Objects

After you create application objects and place them on the directory tree, create the Class-of-Service (CoS) policies that specify the actions you want the switch to take when it detects traffic from those applications.

You can specify different policies for the same application to regulate where and how the traffic for that application flows within the organization.

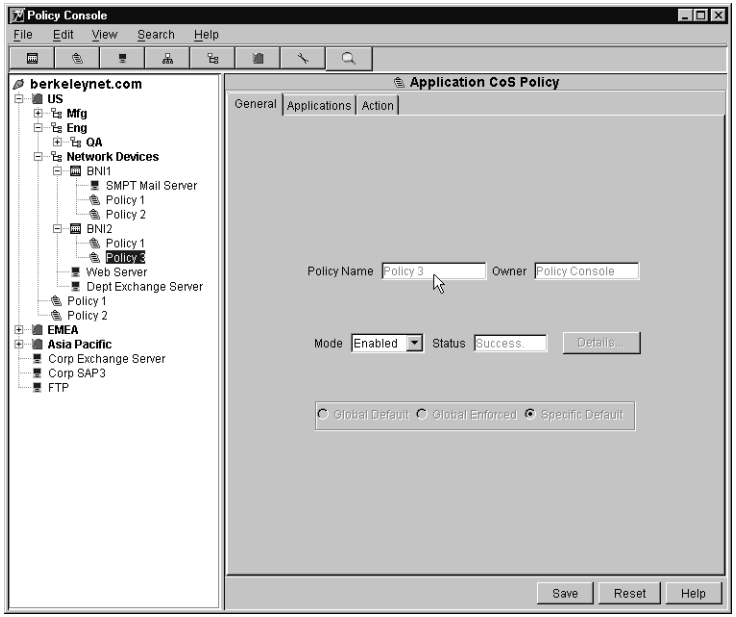
Depending on where you place a policy object and how you configure it, a policy can apply globally, to the corporate network node, or a locality node, or an organizational unit node. Or it can apply specifically to a leaf node representing a department or a switch. *See Chapter 6 for details.*

To create a policy:

1. Select a node–*in the example, US is the first node with a policy subordinate to it.*
2. Click the policy icon on the icon bar to display the Application Policy page.
3. Enter the policy name in the Policy Name field–*in the example, Policy 1 is the first policy under the US locality*.
4. Enter the policy parameters–i*n the example, policies map to applications like this:*

Node	***Policy***	***Node***	***Application***
US	Policy 1	Root	Corp Exchange Server
US	Policy 2	Root	Corp SAP3
BNI1	Policy1	BNI1	SMTP Mail Server
BNI1	Policy2	Net Dev	Web Server
BNI2	Policy1	Net Dev	Dept Exchange Server
BNI2	Policy3	Root	Corp FTP

5. Click Save.
6. Repeat Steps 1–5 for Policy 2.
7. Select the BNI1 switch and repeat Steps 2–5 for Policy=Policy1 and Policy=Policy2.
8. Select the BNI2 switch and repeat Steps 2–5 for Policy=Policy1 and Policy=Policy3.



Note: In the example, six policies were created on the directory tree. *See Step 4 for details*.

Chapter 6–Configuring Policies

This chapter contains a policy overview and provides step-by-step instructions that describe how to configure a policy for FTP–*in the locality-based organization example described in Section 2.4, FTP is one of the applications that exists under the root node.*

Section	***Contents***
6.1	Policy Overview
6.2	Creating an Application Object
6.3	Creating a Policy
6.4	Avoiding and Resolving Policy Conflicts

6.1 Policy Overview

This section provides an overview of application Class-of-Service (CoS) policies and illustrates how these policies work. It describes:

- Functions that policies perform
- Actions that you want a policy to carry out
- Scopes that policies can have–global and specific
- Relationships between applications, policies, and the directory tree.

Policy Functions

Policies specify actions that switches will take when they detect application traffic of a particular type. Policies and applications go together. Before you can implement a policy, you must define an application–*if it is not defined already*.

Policy Actions

Depending on the action you specify for a policy, switches can take one of the following actions when it detects traffic to/from a particular application:

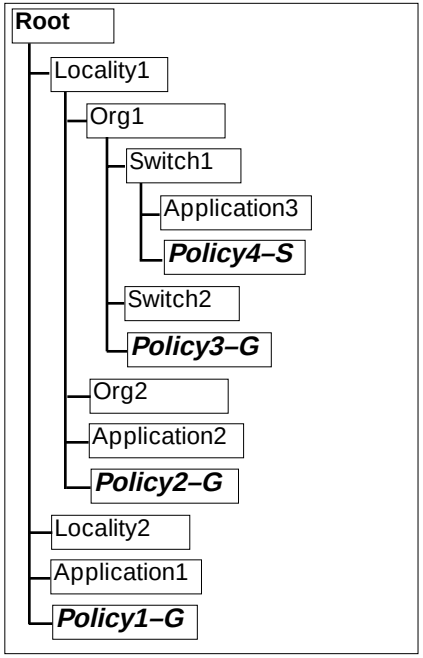
- Raise or lower the priority of that application's traffic–relative to traffic from other applications.
- Drop that application's traffic.
- Redirect that application's traffic to a specific switch port.

Policy Scope–Specific and Global Policies

Policies specify an action and define a scope where the action will be applied. When policies are located above multiple nodes on the directory tree, they will apply to all switches that are directly under them in the directory information tree. When policies are located under one specific switch, they will apply specifically to that switch.

Applications, Policies, and the Directory Tree–*See the Global and Specific Policies diagram.*

If you locate an application object at the root level (*in the example, Application1),* you can create multiple policies for that application (*in the example, Policies 1–4).* Depending on where you position the policy on the directory tree, it will apply to different parts of your organization. A policy applies to all of the nodes on the same level or below where it is positioned.



Global and Specific Policies

Policy	***Applies to:***
Policy1	Root node
Policy2	Locality1
Policy3	Org1
Policy4	Switch1

As shown in the diagram:

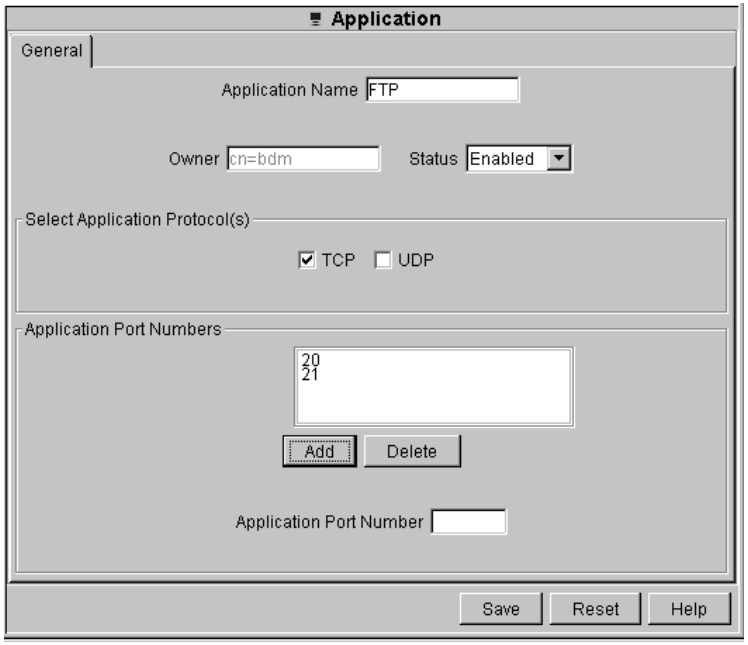
- Policies 1–3 are *global policies* because they are located at nodes with subordinate nodes.
- Policy 4 is a *specific policy* because it is located at a leaf node.

6.2 Configuring an Application Object

Because policies specify actions that switches will take when they detect application traffic of a particular type, policies and applications are linked. A policy requires an application to exist–it must be applied to a specific application.

To create and configure an application object:

1. Highlight a node on the directory tree where you want the policy to apply.
2. Click the application icon on the icon bar to display the Application page.
3. Enter the application name–*FTP in the example.*
4. Select Enabled–*the default setting.*
5. Select the protocol–*TCP in the example*.
6. Enter the application port number(s)–*20 and 21 in the example.*
7. Click Add for each port number you define to have the port number appear in the Application Port Number window.
8. Click Save.

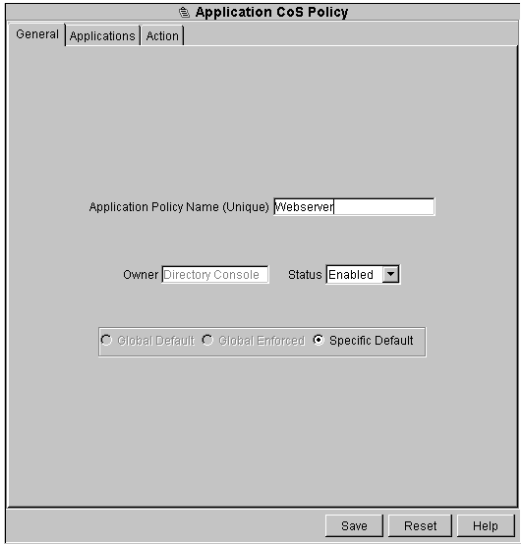


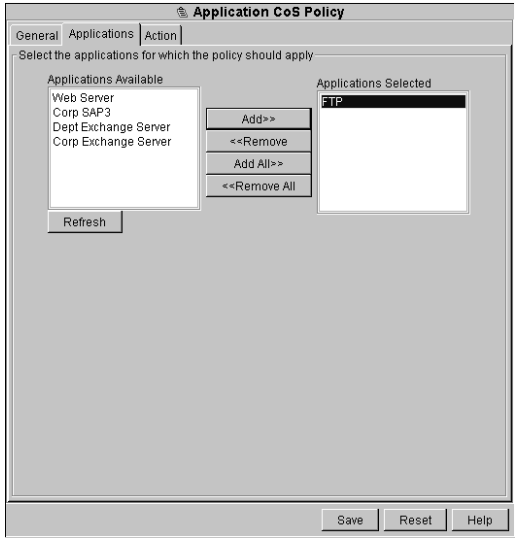
Parameter:	Description
Application Name	Port number of the interface
...Protocol	Protocol the application will run under
...Port numbers	Enter the number of the application **Note:** Well-known applications use standard, reserved numbers. Uncommon applications use numbers that are not reserved.

6.3 Configuring a Policy

To create and configure a policy, highlight a node in the directory tree where you want the policy to apply. Then perform the following steps:

1. Click the policy icon on the icon bar to display the Application CoS Policy General tab page.
2. On the General tab page, enter the policy name *–Webserver in the example.*
3. Select Enabled*–the default setting*.
4. Select the radio button, which defines how you want to apply the policy.
   Note: In the example, FTP was created as a global application, so Global Default and Global Enforced are the options you can select.
5. Click the Applications tab to display the Applications tab page.
6. Click the Refresh button to display the applications you have created in the left window.
7. Select an available application, highlighting it*–in the example, FTP.*
8. Click Add to move the highlighted application, *in the example, FTP,* to the Application Selected window, *the window on the right.*
9. Click the Action tab to display the Action tab page described on the following page.

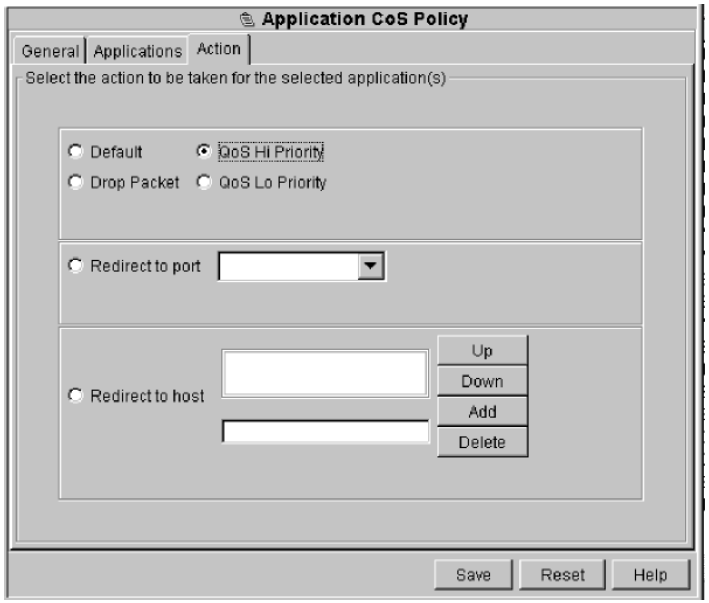




6.3 Configuring a Policy–(continued)

To complete the Configuring a Policy procedure:

10. Click one of the radio buttons on the Action tab page to specify the action you want the switch to take when it receives a packet containing the specified application port number.
11. Click Save to save the policy.



Selection:	Description
Default	Use the default QoS priority that you established at a global level when sending the packet.
Drop Packet	Do not forward the packet.
QoS Hi Priority	When sending the packet, assign it a high priority.
QoS Lo Priority	When sending the packet, assign it a low priority.
Redirect to Port	Forward the packet to the specified port, instead of sending it to the port specified in the packet. *Unused in this release.*
Redirect to Host	*Unused in this release.*

6.4 Avoiding and Resolving Policy Conflicts

This section defines how the order of precedence works for the policies you create. You can create multiple policies for the same application, so it is possible that policies can overlap or conflict. Also, policies that you define using the Policy Console can coexist with policies you define using ESX-Admin.

Certain policies will take precedence over other policies. It depends on:

- How you create those policies–*with ESX-Admin or Policy Console.*
- Where you position those policies on the directory tree.

How Policies Are Created and How They Apply

You can create a policy for an application and specify an action that will apply either globally to multiple switches or specifically to a single switch. In addition, you can create a policy with ESX-Admin or Policy Console.

A policy you create with the Policy Console can apply globally or specifically. A global policy can be either an enforced policy or a default policy. With ESX-Admin, any policy you create will be a specific policy that will apply only to the switch you are connected to when you create the policy. The types of policies are:

- Global Enforced
- Global Default
- Specific–created with the Policy Console
- Specific–created with ESX-Admin

Order of Precedence for Policies

The policies you create observe the following order of precedence:

1. A Global Enforced Policy takes precedence over all other policies.
2. A Specific Policy, whether created using the Policy Console or ESX-Admin, is next in the order of precedence. If specific policies conflict, the first policy created will take precedence.
3. A Global Default Policy will apply if no Global Enforced or Specific policies exist for that application.

Chapter 7–Conducting Directory Server Searches

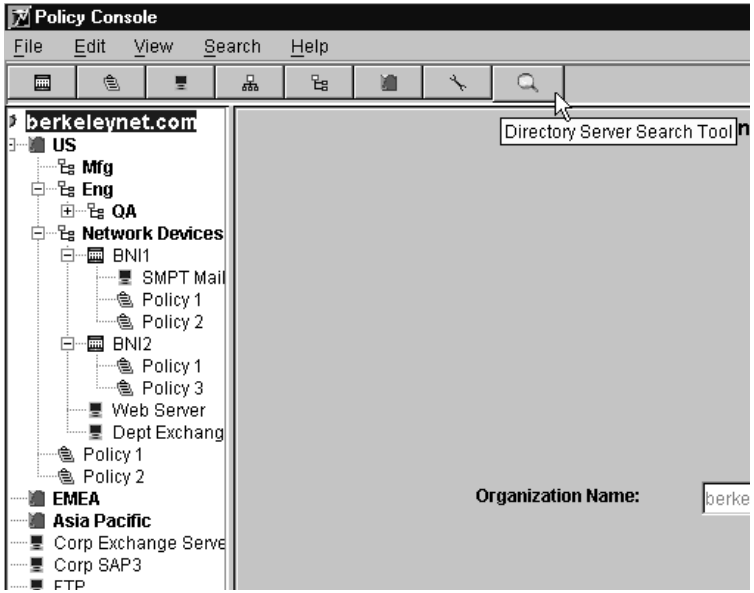
In the event you uncover a policy or a naming conflict, you may need to check the objects located in the Directory Server. This chapter describes how to conduct searches on Directory Server objects using the Search Tool located on the menu bar.

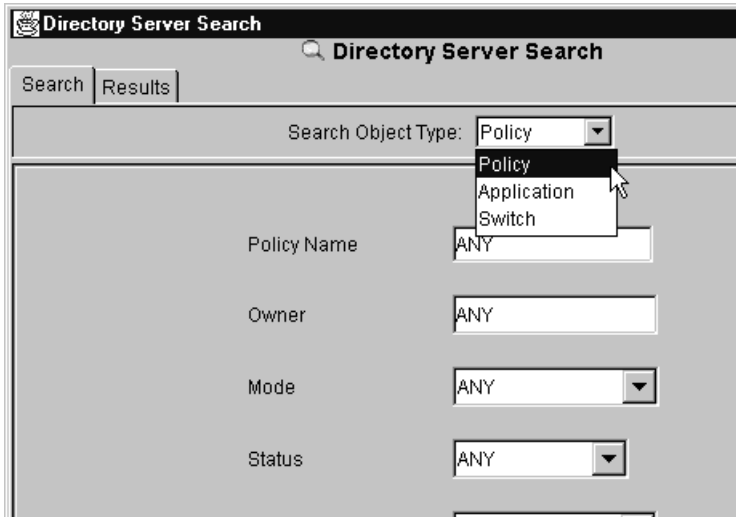
When you click the Search Tool icon, the Directory Server Search window is displayed on the screen. You can select an object type and conduct a search by clicking the Search Object Type window, selecting an object, and specifying parameters for the search.

The following sections describe how to conduct searches for these Directory Server objects.

Section	***Contents***
7.1	Searching for Policiy Objects
5.2	Searching for Application Objects
5.3	Searching for Switch Objects

Note: This chapter describes how to conduct a search on an object located in the sample Directory Tree created in Chapter 5. A search will display information contained in the Directory Server that describes that oject.





7.1 Searching for Policy Objects

This section shows how to Search for a policy object.

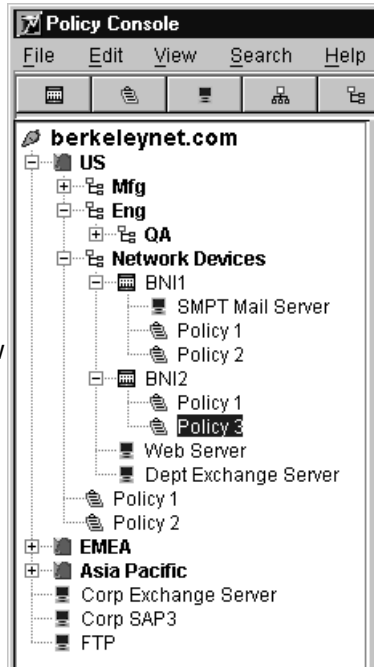
The example shows a search for a policy object (Policy 1) located in the sample Directory Tree.

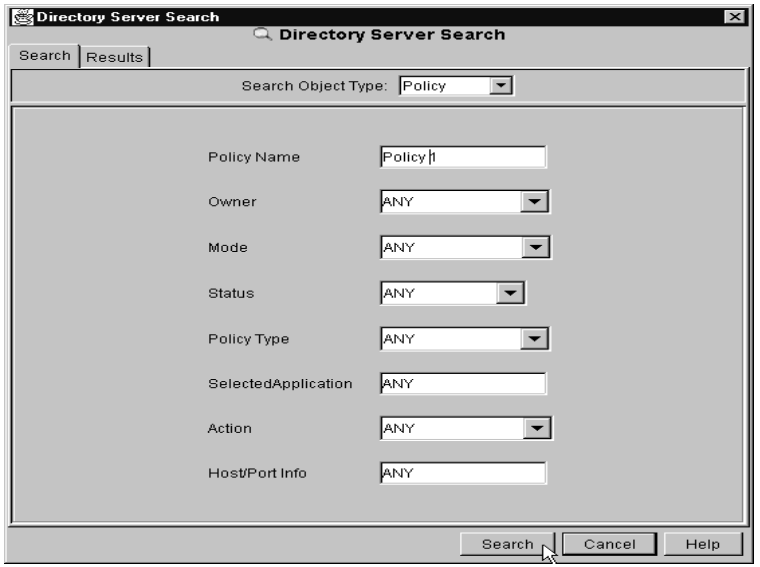
The search displays the results in a window that you can access by clicking the Results tab.

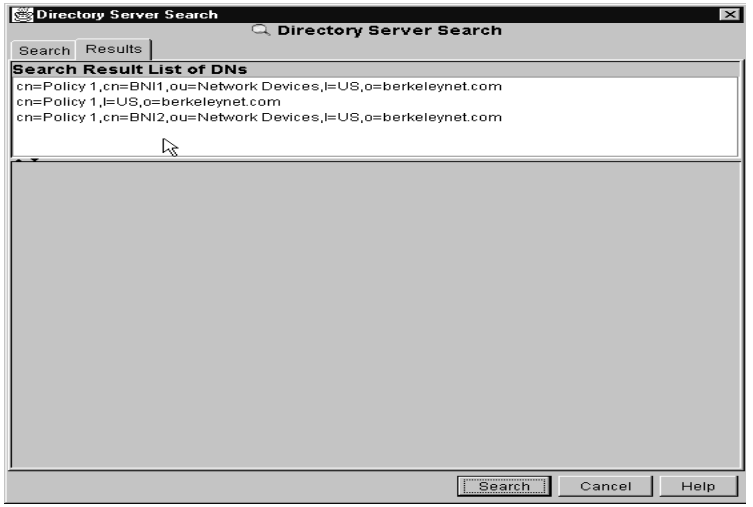
To Search for a Policy Object:

1. Select the Search Tool icon on the menu bar.
2. Select Policy in the Search Object Type window.
3. Specify parameters for the search in the Policy window.
4. Click the Search button.
5. Click the Results tab to view search results.

Note: The search returned three instances of the Policy 1 object in the Directory Server.







7.2 Searching for Application Objects

This section shows how to Search for an application object.

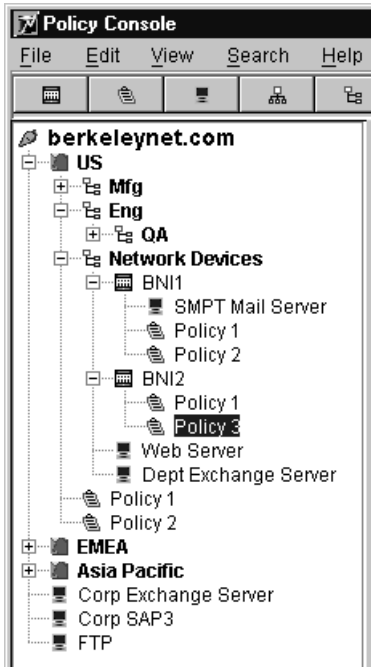
The example shows a search for an application object (Exchange Server) located in the sample Directory Tree.

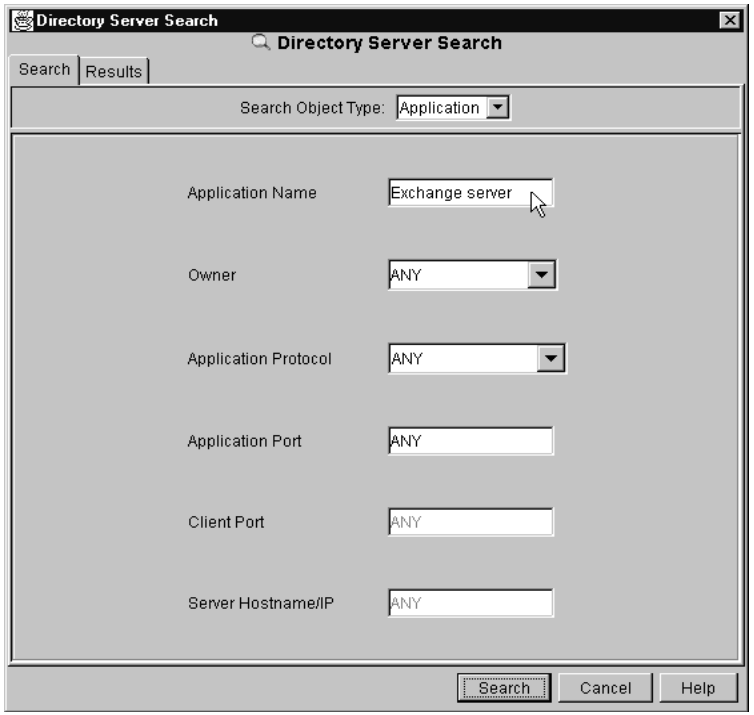
The search displays the results in a window that you can access by clicking the Results tab.

To Search for an Application Object:

1. Select the Search Tool icon on the menu bar.
2. Select Application in the Search Object Type window.
3. Specify parameters for the search in the Application window.
4. Click the Search button.
5. Click the Results tab to view search results.

Note: The search will return two instances of the Exchange Server object in the Directory Server: Corp and Dept Exhange Server.





7.2 Searching for Switch Objects

This section shows how to search for a switch object.

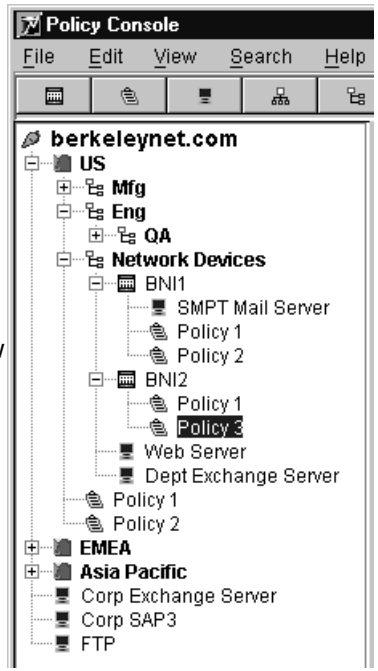
The example shows a search for a switch object (BNI1) located in the sample Directory Tree.

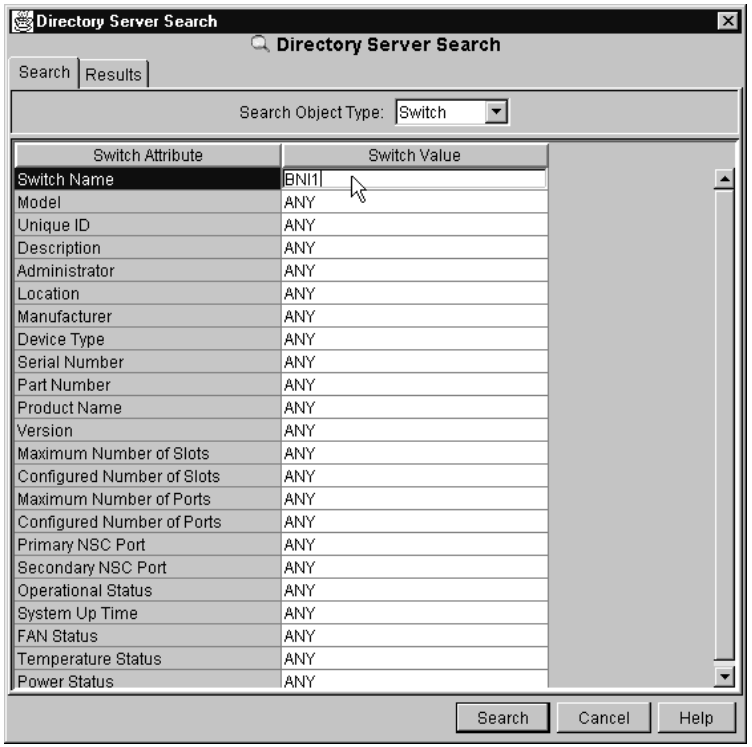
The search displays the results in a window that you can access by clicking the Results tab.

To Search for a Switch Object:

1. Select the Search Tool icon on the menu bar.
2. Select Switch in the Search Object Type window.
3. Specify parameters for the search in the Switch window.
4. Click the Search button.
5. Click the Results tab to view search results.

Note: The search will return one instance of the BNI1 object in the Directory Server.





Chapter 8–ADSA Log Messages

This chapter lists and describes the messages the ADSA log provides. These messages indicate key system events have occurred. To display the ADSA log,enter the following ESX-Cli command:

```
CLI> show log application
```

The ADSA log provides two types of messages:

- *Information Messages* describe system events that are noteworthy, but require no intervention.
- *Error Messages* describe problem conditions. Error conditions may require you to perform a recovery procedure that is contained in the error message description.

8.1 Information Messages ID=2000

The ADSA log displays the following information messages. A description is provided after the message.

ADSA_LOG_DS_CONNECTION_REESTABLISHED
Connection to the directory is re-established.
Note: This message indicates that the directory server went down or that the connection to the directory server was lost.

ADSA_LOG_INIT ADSA service started.

ADSA_LOG_NO_PLUGIN ADSA plugin stopped.

ADSA_LOG_PLG_SHTDWN ADSA plugin stopping.

ADSA_LOG_PLUGIN_INIT ADSA plugin loaded.

ADSA_LOG_STOPPED ADSA service stopped.

8.2 Error Messages ID=3000

The ADSA log displays the following error messages. A description of the probable cause is provided along with a recovery procedure for each probable cause. The recovery procedure is highlighted in italics.

ADSA_LOG_INIT_FAILED ADSA initialization failed.

Probable cause and recovery: ADSA may fail to initialize for one of the following reasons:

- ADSA could not connect to the directory server because you have not configured ADSA correctly using ESX-Cli.
  Verify that ADSA is configured correctly. See Section 3.5, "Configuring Switches to Recognize the Directory Server", for information on how to direct ADSA to connect to the right server using the right credentials.
- There is no network connectivity to the directory server.
  Verify that you can connect to the directory server.
- The registry parameters for ADSA have been misconfigured–this can happen if an upgrade procedure terminates abnormally.
  Verify that the upgrade terminated normally.

ADSA_LOG_DS_SEARCH_FAILED
Directory search failed.

Probable cause and recovery: Check the directory server log file and see why the directory search failed. Error code 81 indicates the directory server is down.

No action is required to start ADSA–it will come up when the directory server comes up.

ADSA_LOG_DS_CONNECTION_FAILED
Failed to connect to the directory server.

Probable cause and recovery: This can happen for one of the following reasons:

- There is no network connectivity to the directory server.
  Verify that you can connect to the directory server.
- The directory server is not running.
  Start the directory server.
  Note: *For NDS, verify that the NLDAP module is loaded.*
- The directory server expects the client to connect to a TCP port other than the default port (port 389).
  Discover the correct port number that the directory expects, and then configure it using this ESX-Cli command:
  `CLI> cfg adsa dport <port-no>`

ADSA_LOG_DS_BIND_FAILED
ADSA failed to bind and authenticate itself to the directory server.

Probable cause and recovery: The correct user DN and password have not been configured on the switch.
Discover the correct user DN and password, and then configure it using this ESX-Cli command:
`CLI> cfg adsa user <user dn> pwd <password>`

ADSA_LOG_PLUGIN_CFG_FAILED
ADSA failed to read the plugin configuration from the registry.

Probable cause and recovery: The NSC registry is corrupted.
Contact FORE Systems Support.

ADSA_LOG_SHT_EVENT_FAILED
Failed to create Shutdown Event Log.

Probable cause and recovery: There may be a problem with NSC kernel.
Contact FORE Systems Support.

ADSA_LOG_PLUGIN_LOAD_FAILED
Plugin load failed.

Probable cause and recovery: The upgrade failed to complete successfully–ADSA did not find the correct plugin DLL.
Perform the upgrade again.

ADSA_LOG_PLUGIN_START_FAILED
Plugin start failed.

Probable cause and recovery: The router is not running.
Start the router.

Probable cause and recovery: You have not set global policies.
Define global policies.

ADSA_LOG_PLGMODIFY_FAILED
The attempt to modify a switch, policy, or application object failed.

Probable cause and recovery: An *ESX-Cli* or *ESX*-Admin client is holding a modify lock for a long time–perhaps the client exited abnormally without releasing the lock.
Stop and Start the router.

ADSA_LOG_PLG_DELREST_FAILED
The plugin DeleteRest failed while attempting to delete an object.
Probable cause and recovery: An ESX-Cli or ESX-Admin client is holding a modify lock for a long time–perhaps the client exited abnormally without releasing the lock.
Stop and Start the router.

ADSA_LOG_PLG_GETOBJ_FAILED
An attempt to get switch policy or application objects failed.

Probable cause and recovery: The router is down.
Start the router.

ADSA_LOG_CREAT_SWITCH_FAILED
ADSA failed to create the switch object in the directory.

Probable cause and recovery: ADSA failed to register the switch object in the directory.
Note: Normally, you will create switch objects in the directory using the Policy Console before you configure ADSA to run on the switches. When you do not perform this optional step, ADSA will detect that the switch object has not been created. It should then create the switch object during its initialization. ADSA can fail to create the switch object for one of the following reasons:

- The switch DN supplied when configuring ADSA through ESX-Cli is incorrect.
  Do not include the name of the switch in the DN.ADSA will put it in automatically during its initialization.
- ADSA does not have sufficient rights to create the switch object.
  Give sufficient rights to the user whose DN is being used by ADSA to log into the directory server.

ADSA_LOG_CFG_GENERAL_BAD
There is a faulty configuration parameter in the ADSA General Parameters section of the registry.

Probable cause and recovery: One or more of the general registry parameters for *ADSA* are either missing or incorrect.
Reconfigure ADSA using ESX-Cli.

ADSA_LOG_DS_RECONNECTION_FAILED
Reconnection attempt to directory server failed.
Note: ADSA will attempt to reconnect every 60 seconds.

Probable cause and recovery: Error log indicates one of the following conditions exist:

- ADSA detected that the directory server has gone down.
- The connection to the directory server has been lost and an attempt to reconnect failed.

Bring up the directory server/fix any connectivity problems.

ADSA_LOG_PLG_OP_FAILED
A particular operation failed in the switch.

Probable cause and recovery: The error code shown below indicates the problem:

Error Code	***Meaning***
1	Cannot get lock on an object. Another client is not releasing the lock. *Stop and Start the router.*
2	Failed to convert a cache object to a directory object.
4	A transient error occurred.
5	Insufficient memory.
19	MIB open failed–*only relevant to switch objects.*
20	MIB operation failed–*only relevant to switch objects*.
21	Cannot get lock on an object. Another client is not releasing the lock. Error is reported only after repeated attempts to get the lock failed. *Stop and Start the router.*

ADSA_LOG_SCC2BDM_OP_FAILED
An LDAP error occurred while updating policy, switch, or application objects.

Appendix A–The ESX DEN Schema Extensions

This appendix lists ESX Attribute and Object Class DEN schema extensions that are loaded when the Policy Console software is installed. When installing a Novell Directory Server, these extensions will appear in NDS. They must be mapped from LDAP to NDS.

LDAP Attribute	NDS Attribute
BNIAction	BNIAction
BNIAdministrator	BNIAdministrator
BNIAppProfileReference	BNIAppProfileReference
BNIAppType	BNIAppType
BNIAssetTrackingNumber	BNIAssetTrackingNumber
BNIAssetType	BNIAssetType
BNICaption	BNICaption
BNIClientPorts	BNIClientPorts
BNICopyRedirSize	BNICopyRedirSize
BNIDestAddrMask	BNIDestAddrMask
BNIDestIPXMACAddrMask	BNIDestIPXMACAddrMask
BNIDestMACAddrMask	BNIDestMACAddrMask
BNIDestPorts	BNIDestPorts
BNIDeviceLocation	BNIDeviceLocation
BNIDevicePortsReference	BNIDevicePortsReference
BNIDeviceReference	BNIDeviceReference
BNIDeviceType	BNIDeviceType
BNIError	BNIError
BNIFanStatus	BNIFanStatus
BNIHLProtocolNum	BNIHLProtocolNum
BNIInstallDate	BNIInstallDate
BNIManufacture	BNIManufacture
BNIMaxNoOfPorts	BNIMaxNoOfPorts
BNIMaxNoOfSlots	BNIMaxNoOfSlots
BNIModel	BNIModel
BNINoOfPorts	BNINoOfPorts
BNINoOfSlots	BNINoOfSlots
BNIOwner	BNIOwner
BNIPDUFlags	BNIPDUFlags
BNIPacketLength	BNIPacketLength
BNIPartNumber	BNIPartNumber
BNIPowerState	BNIPowerState
BNIPrimaryDevicePort	BNIPrimaryDevicePort
BNIPriorityPercentile	BNIPriorityPercentile
BNIProductName	BNIProductName
BNIProtocolType	BNIProtocolType
BNIRemovable	BNIRemovable
BNIReplaceable	BNIReplaceable
BNISKU	BNISKU
BNIScheduleDayOfMonthMask	BNIScheduleDayOfMonthMask
BNIScheduleDayOfWeekMask	BNIScheduleDayOfWeekMask
BNIScheduleMonthMask	BNIScheduleMonthMask
BNIScheduleTimeOfDayRange	BNIScheduleTimeOfDayRange
BNIScheduleValidityPeriod	BNIScheduleValidityPeriod
BNISecondaryDevicePort	BNISecondaryDevicePort
BNISerialNumber	BNISerialNumber
BNISrcIPAddrMask	BNISrcIPAddrMask
BNISrcIPXMACAddrMask	BNISrcIPXMACAddrMask
BNISrcMACAddrMask	BNISrcMACAddrMask
BNISrcPorts	BNISrcPorts
BNIStatus	BNIStatus
BNISvrAddress	BNISvrAddress
BNISvrPortsNDS Attribute	BNISvrPortsNDS Attribute
BNISystemUpTime	BNISystemUpTime
BNITag	BNITag
BNITargetPortReference	BNITargetPortReference
BNITemperatureStatus	BNITemperatureStatus
BNIType	BNIType
BNIVersion	BNIVersion
BNIWeight	BNIWeight

ESX SchemaExtensions {2 16 840 1 113921 1 1}
DEFINITIONS ::=

```
BEGIN
"BNISwitch" OBJECT-CLASS ::=
{
   Operation            ADD,
   Flags
{DS_CONTAINER_CLASS,DS_EFFECTIVE_CLASS},
   SubClassOf           {"Top"},
   ContainedBy          {  "Top",
                        "Country",
                        "Locality",
                        "Organization",
                        "Organizational Unit"
                      },
   NamedBy              {"CN"},
   MustContain          {"CN"},
   MayContain           {
                        "BNICaption",
                        "BNIStatus",
                        "BNIDeviceType",
                        "BNIAdministrator",
                        "BNISerialNumber",
                        "BNIInstallDate",
                        "BNIManufacturer",
                        "BNIDeviceLocation",
                        "BNIModel",
                        "BNIMaxNoOfPorts",
                        "BNIRemovable",
                        "BNIReplaceable",
                        "BNISKU",
                        "BNITag",
                        "BNIVersion",
                        "BNIAssetTrackingNumber",
                        "BNIAssetType",
                        "BNIPowerState",
                        "BNIProductName",
                        "BNIPartNumber",
                        "BNIMaxNoOfSlots",
                        "BNINoOfPorts",
                        "BNINoOfSlots",
                        "BNIFanStatus",
                        "BNITemperatureStatus",
                        "BNISystemUpTime",
                        "BNIPrimaryDevicePort",
                        "BNISecondaryDevicePort"
                      },
   ASN1ObjID            {2 16 840 1 113921 1 2 3}
}
"BNIApplicationProcess" OBJECT-CLASS ::=
{
   Operation            ADD,
   Flags                {DS_EFFECTIVE_CLASS},
   SubClassOf           {"Top"},
   ContainedBy          {  "Top",
                        "Country",
                        "Locality",
                        "Organization",
                        "Organizational Unit"
                      },
   NamedBy              {"CN"},
   MustContain          {"CN"},
   MayContain           {
                        "BNIOwner",
                        "BNIAppType",
                        "BNIProtocolType",
                        "BNISvrPorts",
                        "BNIClientPorts",
                        "BNISvrAddress",
                        "BNIStatus"
                      },
   ASN1ObjID            {2 16 840 1 113921 1 2 2}
}
```

```
."BNIACoSPolicy" OBJECT-CLASS ::=
 {
    Operation           ADD,
    Flags              {DS_EFFECTIVE_CLASS},
    SubClassOf           {"Top"},
    ContainedBy          {  "Top",
                       "Country",
                       "Locality",
                       "Organization",
                       "Organizational Unit",
                       "BNISwitch"
                     },
    NamedBy              {"CN"},
    MustContain          {"CN"},
    MayContain           {
                       "BNIType",
                       "BNIOwner",
                       "BNIAction",
                       "BNIProtocolType",
                       "BNIStatus",
                       "BNIError",
                       "BNIAppProfileReference",
                       "BNIDevicePortsReference",
                       "BNISrcIPAddrMask",
                       "BNIDestIPAddrMask",
                       "BNISrcMACAddrMask",
                       "BNIDestMACAddrMask",
                       "BNISrcIPXMACAddrMask",
                       "BNIDestIPXMACAddrMask",
                       "BNISrcPorts",
                       "BNIDestPorts",
                       "BNIWeight",
                       "BNIHLProtocolNum",
                       "BNIPDUFlags",
                       "BNIPacketLength",
                       "BNIScheduleTimeOfDayRange",
                       "BNIScheduleValidityPeriod",
                       "BNIScheduleMonthMask",
                       "BNIScheduleDayOfMonthMask",
                       "BNIScheduleDayOfWeekMask",
                       "BNITargetPortReference",
                       "BNICopyRedirSize",
                       "BNIPriorityPercentile",
                       "BNIDeviceReference"
                     },
    ASN1ObjID            {2 16 840 1 113921 1 2 1}
 }
 END
```

Glossary

The following key concepts are useful in understanding directory enabled networks:

- **Advanced Directory Services Agent (ADSA)** An extensible software agent that integrates the switch with the directory service and enforces policies. ADSA logs messages to the ADSA log and performs management functions.
- **ADSA Log** A logfile of ADSA messages that can be accessed using the ESX-Cli command:
  `CLI> show log application`
- **Action** A *policy* defines an action to take when it encounters a frame of a certain type. An action can include prioritizing, dropping, or redirecting a frame.
- **Class-of-Service Policy** A policy that defines an *action* to be taken by a network device when it detects traffic classification packets that meet specific conditions in the policy.
- **Policy Console** The workstation connected to the *directory service* that administrators use to manage the network by establishing *policies* and positioning those policies on the *directory tree* to define the behavior of the objects in the network.
- **Directory Enabled Network** An intelligent network that:
  - Stores network resource information centrally in a directory
  - Allows resources to learn about other resources
  - Manages resources via *policies* and the *directory*
- **Directory Tree** The directory organizes *objects* in a hierarchical structure, called a Directory Information Tree (DIT)–sometimes referred to as a directory tree. The directory tree has an inverted tree shape.
- **Directory Server** A stand-alone server hosting the *directory service* software that communicates with switches in the network and the *Policy Console* using the LDAP protocol.
- **Directory Service** The repository of information describing the network, its resources, and the relationships among these resources.
- **Distinguished Name (DN)** The differentiated, or qualified, name of a node–starting with the relative name of the node and going back to the root.
  The distinguished name of Switch1, for example:
  CN=Switch1, OU=Manufacturing, L=West Coast, O=Acme.com.
  where: Switch1=the relative name of the switch
- **Enforcement** Underlying DEN is the ability to enforce a *policy* after it has been created either at a global or at a specific level. Enforcement is done at the switch level where all collisions are detected and resolved.
- **Filter** A *policy* uses a filter that examines the frame header to detect if a condition exists. Filters can be set to look for specific applications, protocols, hosts, or ports.

- **Frame Header** The first part of the frame that contains information describing the contents of the frame, including:
  - Source address
  - Destination address
  - Application ports
  - Protocol type
- **Global Policy** A policy for an application, or group of applications, that is implemented on multiple nodes in a network.
- **Inheritance** DEN uses inheritance to propagate a *policy* throughout the network after this policy has been created. This mechanism is used to create global policies that apply to the entire network or a group of devices. Inheritance is always executed top-down.
- **LDAP** Lightweight Directory Access Protocol is a directory access standard originally implemented by the University of Michigan. V3 is the latest version. It is defined in RFC 2251.
- **Objects** The *Policy Console* represents elements in the network as objects belonging to one of these classes:
  - Geographic region (or locality)
  - Organizational unit
  - Switch
  - Application
  - Application policy
- **Policy** The *Policy Console* lets you specify a policy or course of action for an application. You then assign this policy to a switch or group of switches to enforce. A policy consists of a set of *filters* and *actions.*
- **Root Node** The top of the tree is referred to as the root node. Network objects are arranged under the root node.
- **Switch** An ESX switch–a layer-4, application-aware, networking device.